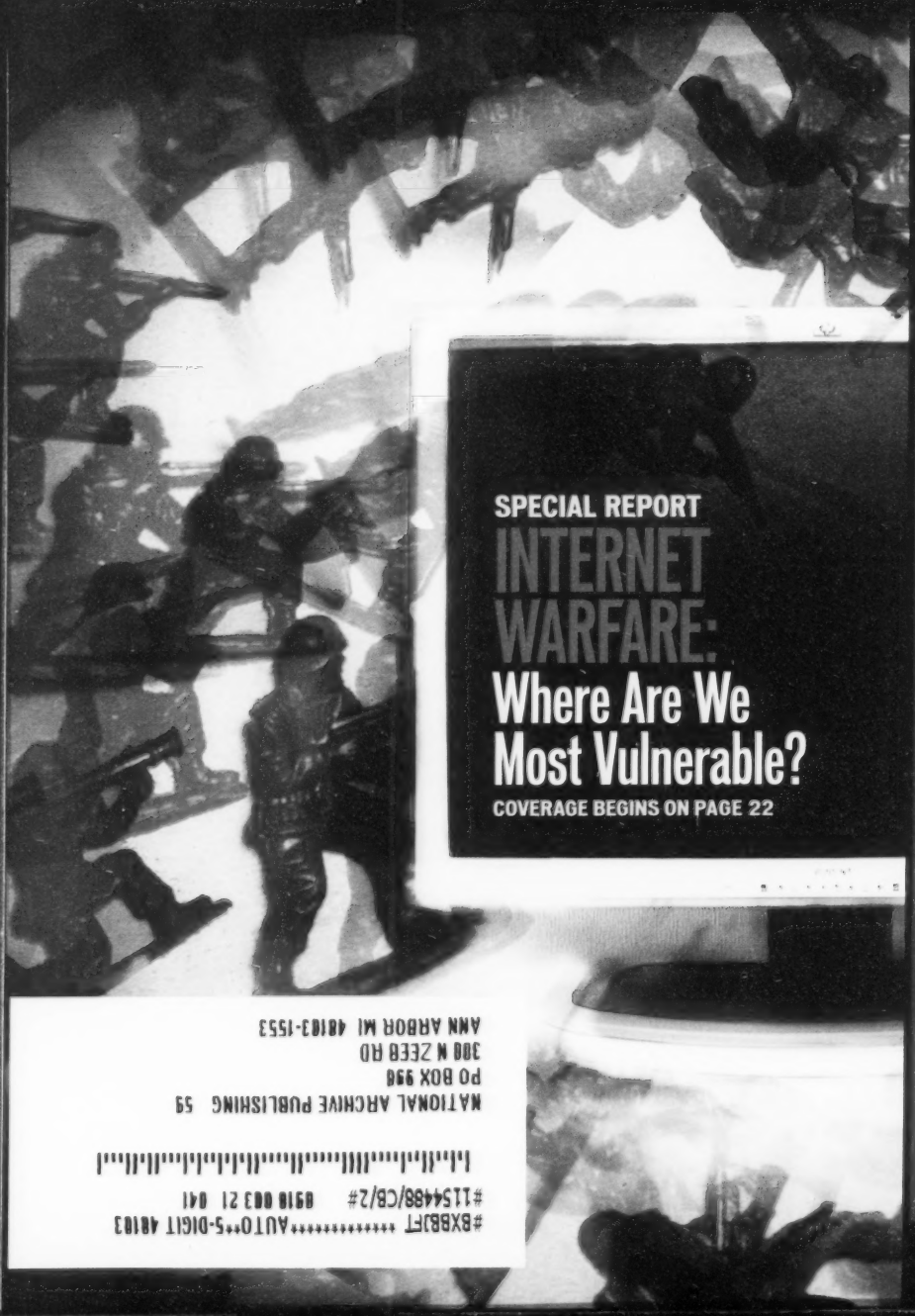
THE GRILL: Networking visionary Rob Faludi talks about monitoring energy consumption and introducing your toaster to your smoke alarm. PAGE 18

COMPUTERWORLD®



SPECIAL REPORT

INTERNET WARFARE: Where Are We Most Vulnerable?

COVERAGE BEGINS ON PAGE 22

#BXBBJFT ********AUTO**5-DIGIT 48183
#1154488/CB/2# 8918 003 21 041
NATIONAL ARCHIVE PUBLISHING 59
PO BOX 998
308 N ZEEB RD
ANN ARBOR MI 48103-1553

Inside

MAY 4, 2009
VOL. 43, NO. 17 $5/COPY

News & Analysis

SAP slows down price increases on software support. But they're still coming. PAGE 10

IT managers prep for a possible pandemic amid budget cutbacks and layoffs. PAGE 14

The time has come for wireless apps to play a big role in health care – if proponents are right. PAGE 16

Opinion

Recognize these five signs that your IT project is in trouble – before it's too late to fix it. PAGE 36

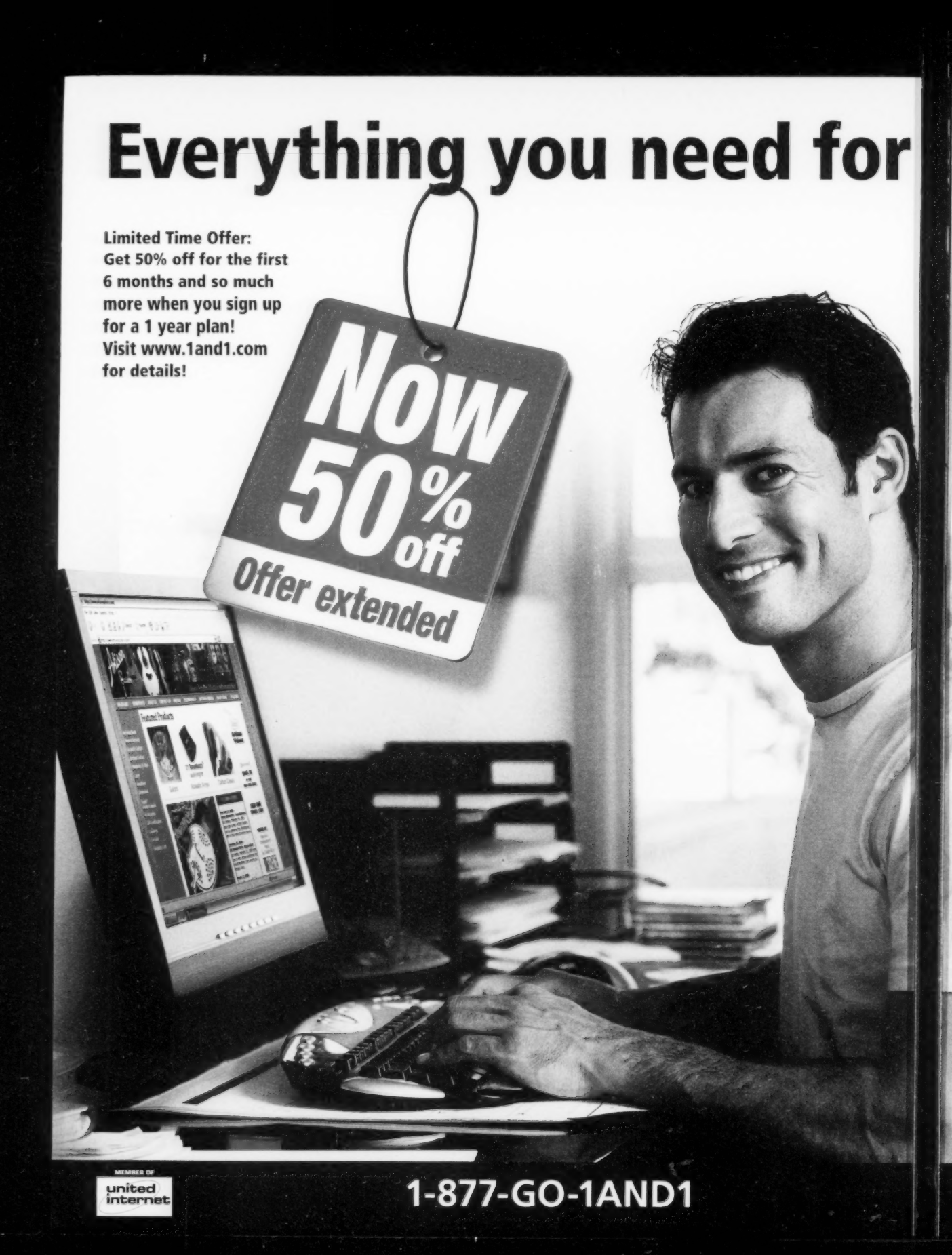
Careers

An IT training firm is offering special deals to unemployed workers. PAGE 37

Don't Miss . . .

When someone says, 'The Internet is down,' what does that really mean? PAGE 34

COMPUTERWORLD.COM


Everything you need for
Limited Time Offer:
Get 50% off for the first
6 months and so much
more when you sign up
for a 1 year plan!
Visit www.1and1.com
for details!
Now
50% off
Offer extended
MEMBER OF
united internet
1-877-GO-1AND1

a successful website

DOMAINS

NEW Savings!

Reserve your unique web address today and save. Protect your personal information. Private domain registration, a 2 GB e-mail account, domain forwarding and a starter website-building tool are included for FREE!

.info
$0.99 FIRST YEAR*

.com .net .org .us
~~$8.99/year~~
$6.99 FIRST YEAR*

Now on sale!

WEB HOSTING

Everything you need for a professional website. 1&1 WebsiteBuilder, 1&1 E-mail Marketing Tool, Mailing List, Driving Directions, Photo Gallery, 1&1 Blog and more! Search advertising vouchers are included with all plans!

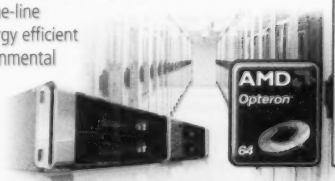
1&1 BUSINESS PACKAGE
- 3 domain names
- 2,500 e-mail accounts
- 250 GB web space/ 2,500 GB monthly transfer volume

~~$9.99/month~~
$4.99 PER MONTH* (first 6 months)

Now 50% off
Offer extended

PREMIUM SERVERS

Designed specifically for high performance needs. Our premium servers feature top-of-the-line AMD Opteron™ processors with energy efficient technology, reducing costs and environmental impact with increased performance-per-watt. 1&1 matches 100% of the energy consumed in our data center with Renewable Energy Certificates.



1&1 BUSINESS SERVER II
- Dual-Core Opteron™ Processor 1218
- 2 x 2.6 GHz, 4 GB DDR RAM, 2 x 500 GB hard drive
- RAID 1 included for FREE!

~~$199.99/month~~
$99.99 PER MONTH* (first 6 months)

Now 50% off
Offer extended

Now accepting PayPal

THIS COMPANY USES CERTIFIED CLEAN ENERGY

*Offers valid for a limited time only. Private domain registration not available with .us domains. Server prices based on Linux servers. Setup fee, minimum contract term, and other terms and conditions may apply. Visit www.1and1.com for full promotional offer details. Program and pricing specifications, availability and prices subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet AG, all other trademarks are the property of their respective owners.
© 2009 1&1 Internet, Inc. All rights reserved.

1&1

www.1and1.com

NEWS

10 User groups persuade **SAP** to extend the **phase-in** period for higher software **support fees.** | **IBM** unveils a new **supercomputer** designed to let it compete with humans on the TV game show **Jeopardy.**

11 A Microsoft **Windows 7 tool** that lets users run **Windows XP** apps in a **virtual machine** could create support nightmares, analysts warn. | **Sun** reports another sharp **drop in quarterly revenue.**

12 **Critics** are raising questions about growing calls for the **White House** to play a leading role in coordinating **cybersecurity efforts** for the government and key private-sector industries.

14 **IT Faces Possible Pandemic Amid Budget Cutbacks.** Decreased funding and layoffs present a challenge to IT managers who must take steps to deal with a possible flu pandemic.

16 **Wireless IT in Health Care: The Time Is Now?** Proponents of wireless health-care technology think it's ready for a takeoff in adoption. But is that a sound prediction or a case of cockeyed optimism?

OPINION

6 **Don Tennant** is perturbed by the level of disagreeableness that people exhibit when they disagree over things like the iPhone Baby Shaker app.

36 **Paul Glen** says that although it's true that the recession is killing a lot of projects, yours may be dying of natural causes.

40 **Frank Hayes** sets the record straight on swine flu: The pandemic panic peddlers have things backward.

DEPARTMENTS

18 Networking expert **Rob Faludi** wants to introduce your toaster to your smoke alarm and help you bond with your plants.

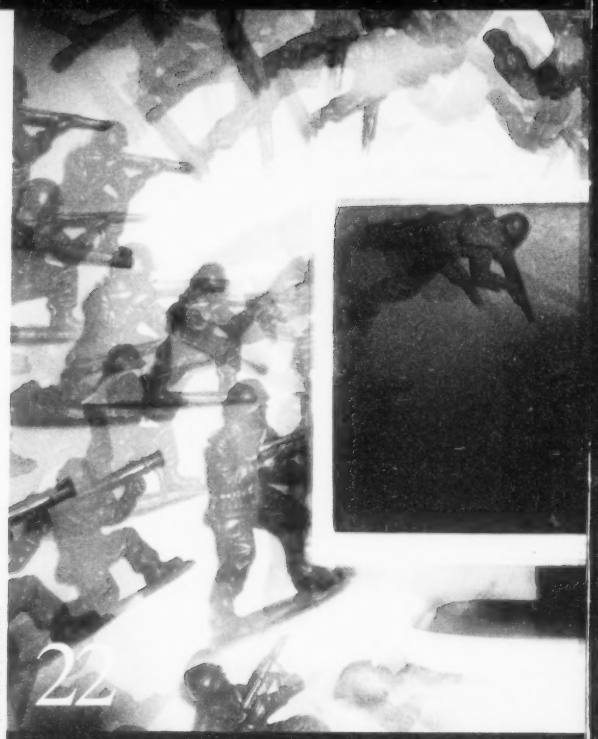
35 **In the Trenches, as the Threats Evolve.** We've gone from free-floating malware to targeted attacks to organized international crime. What will be next?

37 Are layoffs too expensive? One researcher says they could be.

39 Read about a manager who *really* supports her employees.

ALSO IN THIS ISSUE

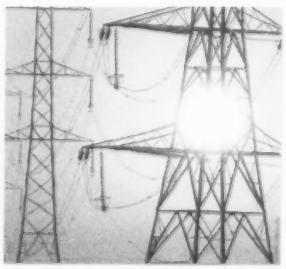
Online Chatter 8
Company Index 39



■ SPECIAL REPORT

INTERNET WARFARE: Where Are We Most Vulnerable?

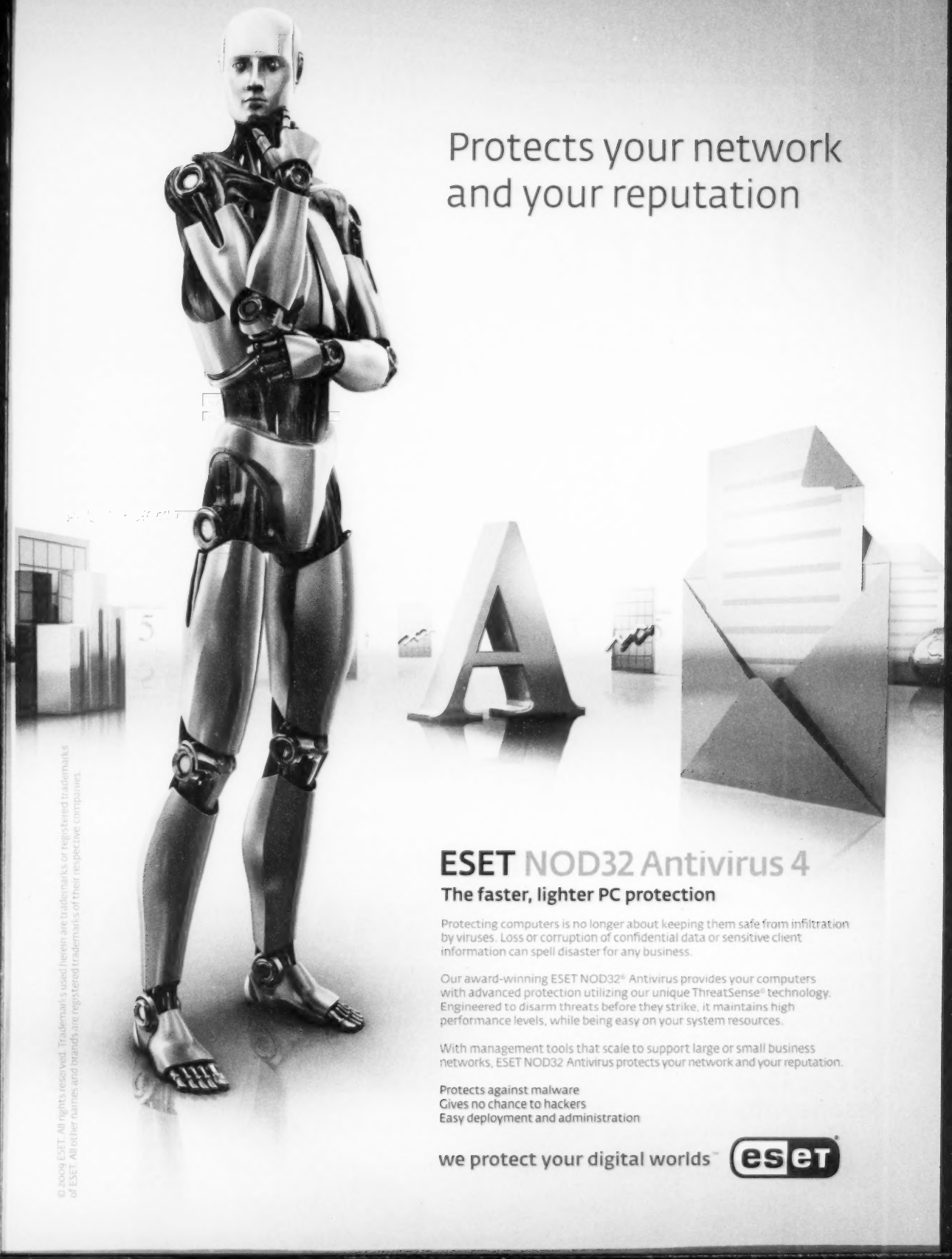
22 Software: The Eternal Battlefield
Most attacks against computer systems exploit software weaknesses. The old protections are no longer enough.



30 New Ground Zero: The Electric Power Grid
Experts agree that the electric power grid is the piece of the critical infrastructure that's most vulnerable to attack.

33 Russia's Cyberblockade Of Georgia Worked
Lesson learned: DDoS attacks – and the responses to them – can cripple a country. Could it happen in the U.S.?

34 'The Internet Is Down.' What Does That Really Mean?
The Internet is still there – we just say it's "down" because we can't get to it. The question is, *why* can't we get to it?


Protects your network
and your reputation
ESET NOD32 Antivirus 4
The faster, lighter PC protection
Protecting computers is no longer about keeping them safe from infiltration by viruses. Loss or corruption of confidential data or sensitive client information can spell disaster for any business.
Our award-winning ESET NOD32® Antivirus provides your computers with advanced protection utilizing our unique ThreatSense® technology. Engineered to disarm threats before they strike, it maintains high performance levels, while being easy on your system resources.
With management tools that scale to support large or small business networks, ESET NOD32 Antivirus protects your network and your reputation.
Protects against malware
Gives no chance to hackers
Easy deployment and administration
we protect your digital worlds™
eset
© 2009 ESET. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET. All other names and brands are registered trademarks of their respective companies.

COMPUTERWORLD.COM

This Week Online

FIND THESE STORIES AT COMPUTERWORLD.COM/MORE

© EISENHANS/FOTOLIA.COM

Noncompetes Done Right

Don't sign away your future. You do have rights. Just know what you're signing and what your employer is really trying to protect.

Jawbone Prime Headset

REVIEW: The latest iteration of Aliph's Bluetooth headset is lightweight, stylish and efficient.

15 Easy Fixes for Mac Security Risks

How safe is your Mac? Maybe not as safe as you think. Here are some quick ways to beef up security.

Blog Spotlight

iPhone Customers Unlikely to Stray

Apple recently sold the 1 billionth iPhone app. Now that they're hooked, Apple's mobile customers are less apt to be tempted by Microsoft's upcoming ZuneHD, Seth Weintraub suggests.

Too Many Desktop Linuxes?

Steven J. Vaughan-Nichols is a big Linux fan, but even he admits that the market may be too segmented. The list of desktop Linuxes goes on and on, and maybe that's one of its biggest problems.

PRIVACY-INFORMATION SERVICES: The Free, the Cheap and the Pricey

Those who need to keep their companies compliant with privacy regulations around the world can find sources of information to fit any budget.

Hackers Need Not Apply

General Dynamics should have known better than to run a "hackers wanted" ad. Ira Winkler wants to know why anyone would think that hackers can do a security professional's job.

Windows 7 RC1

REVIEW: Microsoft's next OS is fast and has UI improvements – plus some truly weird wallpaper.

Windows 7 on a Netbook

HANDS ON: Microsoft has said that any version of Windows 7 will run on a netbook. We try it with Windows 7 Ultimate.

SHARK BAIT

Computer Possessed by Galactic Signals

An industrious employee is surprised one day to find his computer performing sensor sweeps of nearby star sectors. It wasn't a screensaver, he insists, and he doesn't have SETI@Home installed. Has he entered The Twilight Zone?

ONLINE DEPARTMENTS

Breaking News	computerworld.com/news
Newsletter Subscriptions	computerworld.com/newsletters
Knowledge Centers	computerworld.com/topics

Proven Success

SAS and 1-800-FLOWERS.COM

"With SAS® business analytics we've been able to increase our customer repeat rate from 40 to 50 percent."

Steve Bozzo | CIO
1-800-FLOWERS.COM

Find out how
www.sas.com/grow

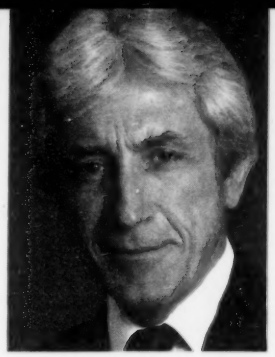
sas | THE POWER TO KNOW.

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. © 2009 SAS Institute Inc. All rights reserved. 35144US.0409

■ EDITOR'S NOTE

Don Tennant

Blaring the Horn



QUESTION: What's the difference between Windows Vista and the infamous Baby Shaker application? Answer: One is an abomination that epitomizes everything that's wrong with the garbage that clueless software developers are dumping on consumers of technology. The other runs on an iPhone.

Now, if that offended you, at least hear me out. I'm just trying to make a point. Let's start with the sick Baby Shaker app that Apple approved for its iPhone but later removed from its store.

As I wrote in my blog last week, I don't pretend to fully comprehend the hurt and anguish felt by parents of children who have been harmed by shaken baby syndrome, but I do share their outrage. So I welcomed the fact that Apple issued a statement of apology, acknowledging that the app was "deeply offensive and should not have been approved for distribution." And I was pleased to see that Sikalosoft, the developer of the application, stated on its Web site that it was "a bad idea . . . that was greatly lacking in taste." It advised consumers that "there are many other iPhone applications you could be better spending your time and money on."

Less satisfied with those statements was the Sarah Jane Brain Foundation, an organization that does wonderful work on behalf of families that suffer from the consequences of shaken baby syndrome. Certainly the Baby Shaker app controversy presented a valuable opportunity to educate the public, and the foundation was right to seize it. But the way it went about it was disappointing.

Instead of launching an intensive information campaign with the Baby Shaker controversy as the door-opener, the foundation reacted like a surly driver with road rage. It launched an attack against Apple and AT&T, presenting a list of demands to the boards of directors of the two companies. The foundation warned that if the companies failed to meet its demands — which included "a complete accounting as to who was responsible for the vetting and launching of this sick application" and the development of "a significant plan to reverse the damage they have caused" — it would hold demonstrations in front of Apple stores in 15 cities.

■ We need to be more tolerant so that we can focus on addressing the serious matters that confront us.

Keep that in mind as we turn to a separate incident that occurred last week, involving Windows Vista. A reader e-mailed me in response to an opinion piece by *Computerworld* columnist and blogger Steven J. Vaughan-Nichols titled "Microsoft Is Doing Something Half Right." The reader was offended by Vaughan-Nichols' statement, "No one with two brain cells wants Vista."

"Since you are where the buck stops at *Computerworld* I am going to assume you approved this statement," the reader wrote, expressing the view that the statement is "insulting" to readers. "What the hell are you thinking?"

I explained to the reader that the editorial buck actually stops with Scot Finnie, our editor in chief, but that the editorial management couldn't possibly approve every statement in every opinion piece, nor would it be inclined to do so. I added for clarity that if the column had been submitted to me for approval, I would have unhesitatingly signed off on it. "Bloggers and columnists need to be free to express their opinions without being concerned about running afoul of the editorial leadership," I wrote.

Again, what surfaced seemed akin to road rage. This reader, the president of a software vendor in Granite Bay, Calif., responded by informing me that "computerworld.com is now blocked at our company firewall and the receptionist who delivers the mail has been instructed to dispose of any *Computerworld* magazines that arrive." I don't know how many employees the company has, but unilaterally forbidding them to read *Computerworld* at work because of a statement written by one of our columnists, and my support of him, doesn't accomplish much.

We need to lighten up, and we need to be more tolerant of one another so that we can focus on addressing the serious matters that confront us. Blaring the horn gets us nowhere. ■

Don Tennant *is* Computerworld*'s senior editor-at-large. You can contact him at don_tennant@computerworld.com, visit his blog at* http://blogs.computerworld.com/tennant, *and follow him on Twitter at* http://twitter.com/dontennant.

Give your company the flexibility to adapt to any business environment.

Converged Solutions from Sprint uses a flexible IP core for your company's voice, video and data communications. With technology like Wireless Integration, your mobile has all the functions of your desk phone. So you and your workforce can adapt to just about every situation you find yourself in. Get it on the Now Network.™

sprint.com/convergence

cisco Powered — Certified by Cisco for Quality of Service

Sprint

©2009 Sprint. Sprint and the logo are trademarks of Sprint. Other marks are the property of their respective owners.

COMPUTERWORLD

P.O. Box 9171, 1 Speen Street
Framingham, MA 01701
(508) 879-0700
Computerworld.com

■ **EDITORIAL**

Editor in Chief Scot Finnie

Senior Editor-at-Large Don Tennant

Executive Editors Mitch Betts, Julia King (events)

Managing Editors Michele Lee DeFilippo (production), Sharon Machlis (online), Ken Mingis (news)

Design Director Stephanie Faucher

Director of Blogs Joyce Carpenter

Technologies Editor Johanna Ambrosio

Features Editors Kathleen Melymuka, Valerie Potter, Ellen Fanning (special reports), Barbara Krasnoff (reviews)

Senior Editor Mike Barton (new media)

Senior News Editor Craig Stedman

News Editors Mike Bucken, Marian Prokop

National Correspondents Gary Anthes, Julia King, Robert L. Mitchell

Reporters Sharon Gaudin, Matt Hamblen, Gregg Keizer, Eric Lai, Lucas Mearian, Patrick Thibodeau, Jaikumar Vijayan

Features Writer, Video Editor David Ramel

Assistant Managing Editor Bob Rawson (production)

Senior News Columnist Frank Hayes

Art Director April Montgomery

Research Manager Mari Keefe

Senior Copy Editors Eugene Demaitre, Monica Sambataro

Copy Editor Donna Sussman

Associate Editor, Community Ken Gagné

Office Manager Linda Gorgone

Contributing Editors Jamie Eckle, Preston Gralla, Tracy Mayor

■ **CONTACTS**

Phone numbers, e-mail addresses and reporters' beats are available online at *Computerworld.com* (see Contacts link at the bottom of the home page).

Letters to the Editor Send to letters@computerworld.com. Include an address and phone number for immediate verification. Letters will be edited for brevity and clarity.

News tips newstips@computerworld.com

Subscriptions and back issues (888) 559-7327, cw@omeda.com

Reprints/permissions The YGS Group, (800) 290-5460, ext. 148, computerworld@theygsgroup.com

■ ONLINE CHATTER

RESPONSES TO:

Why I Use Linux

April 21, 2009

I don't get why people writing articles on the Internet constantly have to write this rubbish about why they love Linux and why everyone should switch to it.
■ **Submitted by:** *Anonymous*

Microsoft pushes its beliefs (valid or otherwise) at me all the time with advertising and marketing. Why shouldn't people who prefer a (frankly better) computer experience let others know about it? The worst that could happen is that Microsoft might improve its operating system — compete on merit, that kind of thing.
■ **Submitted by:** *David Freehug*

RESPONSES TO:

Don't Sign Away Your Future: Noncompetes Done Right

April 23, 2009

The author assumes you have a choice. I have been forced to sign these "indentured servant" agreements. Sometimes doing so is "suggested," other times you are flat-out told, "If you don't sign, go home."

The unemployment rate for IT workers is 12% in my area — and given the Department of Labor's distorted data collection, it's more like 22% in reality.
■ **Submitted by:** *Ann*

I worked for a small company that was bought out by a Fortune 500 company. During the transition process I was given a choice of signing a new noncompete or not having a job. The agreement I signed is so extensive that it basically says I can't earn a living after I leave. It angered me at the time, but at this point I am not concerned about it being enforced because of how extreme it is.
■ **Submitted by:** *Anonymous*

The first company I worked for implemented a noncompete clause for sales staff that prohibited them from working in computer sales for any other company for a year. To make things worse, this company was going down the tubes at the time. Some salespeople were able to jump ship, but it was 1987, around the time of the big Dow Jones crash, and sales jobs were about as plentiful as they are now — meaning people were happy to have a job. Many of these people were specialized in computer hardware and good at it. Sure, they could have started selling insurance or something, but that would have been a waste of their talents.
■ **Submitted by:** *Aardvark*

A contract that benefits only one side is not a contract! Slavery was made illegal in the U.S. some years ago.
■ **Submitted by:** *Dr Bob Hacker*

RESPONSE TO:

#amazonfail

April 20, 2009

I'll bet Amazon was trying to do just what Frank Hayes suggests. The problem is that a system as big as Amazon's has trouble communicating over all its farflung parts, so when a problem crops up, everybody decides it's "their" problem and responds as best they can with their limited info.

It's an unsolvable dilemma. If you centralize things so that only PR can speak for the company, you get leaks and delays and PR-speak. If you decentralize, you get the "blind men and elephant" descriptions we had here. Somebody should build a software tool to help internal communications, you know, so they could build a . . . um . . . social network.
■ **Submitted by:** *Eadwacer*

JOIN THE CHATTER! *You, too, can comment directly on our stories, at* **computerworld.com.**

LEANER.
MEANER.
GREENER.
The inefficiency, complexity and rising energy costs of twentieth-century datacenters simply can't support the demands of twenty-first-century business. The IBM BladeCenter® HS22 with Intel® Xeon® Processor 5500 Series can improve the economics of your datacenter by using up to 95% less space and 90% less energy than competitive rack servers deployed 3 years ago, all without sacrificing performance.[1] A greener world starts with greener business. Greener business starts with IBM.
SYSTEMS. SOFTWARE. SERVICES. FOR A GREENER WORLD.
Learn how to improve performance and costs at ibm.com/green/bladecenter
IBM
intel
Xeon
inside
Powerful.
Intelligent.
[1]For complete details, go to www.ibm.com/green/disclaimer. IBM, the IBM logo, ibm.com and BladeCenter are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml. Intel, the Intel Logo, Xeon and Xeon Inside are trademarks or registered trademarks of Intel Corporation in the United States and other countries. © 2009 IBM Corporation. All rights reserved.

News Digest

FIND THE FULL STORIES AT
COMPUTERWORLD.COM

THE WEEK AHEAD

MONDAY: Collaborate 09, a conference held jointly by three independent Oracle user groups, opens in Orlando. Also starting today is RailsConf 2009, an event in Las Vegas focusing on the Web development framework Ruby on Rails.

TUESDAY: Microsoft plans to make the "release candidate" version of Windows 7 broadly available; it released the software to its MSDN and TechNet subscribers last week.

WEDNESDAY: Cisco plans to report its third-quarter results.

ENTERPRISE SOFTWARE

SAP Slows Price Hike on Forced Support Switch

BOWING TO pressure from user groups, SAP AG last week agreed to slow the pace at which its software support fees will increase under the mandatory Enterprise Support program that the vendor launched last year.

SAP and representatives from 12 user groups also announced a series of key performance indicators, or KPIs, that they have agreed upon for attempting to measure Enterprise Support's financial value to customers.

The forced switch to Enterprise Support has been a bone of contention ever since it was announced. In an initial attempt to appease angry customers last fall, SAP sweetened some of the program's features and extended the regular maintenance period for its core business applications from five years to seven. But the company didn't make any cost concessions then.

And last week, SAP said the ultimate price of Enterprise Support will still amount to 22% of software license fees annually. The company charged a 17% fee for its Standard support program, one of two lower-cost offerings that it eliminated.

But instead of applying the increase in four annual steps ending in 2012, SAP will now extend the phase-in period to seven years. As a result of the change, SAP said, support costs for migrated customers will rise by an average of 3.1% each year, instead of the 8% that users originally faced.

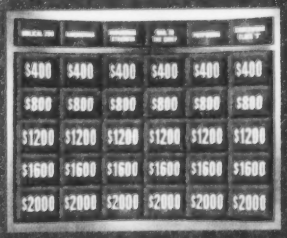
Reducing the annual rate of increase was one of the demands made by SAP's user groups. The list of KPIs that SAP and the user groups agreed on resolves another demand: finding a common way to assess the value of Enterprise Support.

SAP claims that the price increase will be justified by improved services, but the user groups want proof. To try to get it, the KPIs will be used in a joint benchmarking program, with the results to be examined by an independent auditor.

The deal isn't perfect, said the Francophone SAP Users' Club. But the group added that it is satisfied with the price-increase compromise. It also said that the agreement on the KPIs shows a willingness on SAP's part to go where no other software vendor has ventured before.

During a conference call on SAP's first-quarter results last week, co-CEO Leo Apotheker made a similar point and maintained that Enterprise Support "will become a competitive advantage" for the company.

— Peter Sayer and Chris Kanaracus, IDG News Service



SUPERCOMPUTING

IBM Plans Human-Machine *Jeopardy* Match

IBM last week unveiled an advanced computing system that engineers hope can compete against humans on the long-running television game show *Jeopardy*.

The system, known as Watson, runs new software called Question Answering (QA), which was designed to understand complex questions and to answer them quickly enough to compete on a rapid-fire show like *Jeopardy*, according to IBM.

David Ferrucci, who heads the Watson project team, said QA's developers were faced with the challenge of developing a supercomputer that "can rival the human mind's ability to determine precise answers to natural-language questions."

An IBM spokesman would not identify the processor that will run the Watson machine, nor would he say how fast it will be able to process data.

– SHARON GAUDIN

OPERATING SYSTEMS

Virtual XP Mode Could Cause Support Woes

A NEW Microsoft add-on for Windows 7 that will let some users run Windows XP applications in a virtual machine could create support nightmares for IT managers, analysts said last week.

The company had announced last month that the add-on, called Windows XP Mode (XPM), will be available to users of the Windows 7 Professional, Ultimate and Enterprise versions once the new operating system ships later this year. Professional and Ultimate are the two highest-priced versions of Windows 7, while Enterprise is sold only through volume licensing agreements.

Analysts agreed that Microsoft needs to offer the add-on to help persuade users to upgrade to Windows 7, but they also noted that it could cause multiple problems for corporate users.

"This will help the uptake for Windows 7, because it removes one more gotcha, and that's never a bad thing to do," said Michael Cherry, an analyst at Directions on Microsoft.

> **"Businesses don't want to support two instances of Windows on each machine.**
>
> **MICHAEL SILVER,** ANALYST, GARTNER INC.

Cherry added that Microsoft's decision to use virtualization to provide backward compatibility is a nice "safety net" for users who lack access to Microsoft's Enterprise Desktop Virtualization technology.

Michael Silver, an analyst at Gartner Inc., echoed Cherry's take on what motivated Microsoft to offer XPM, but he added that it broadly expands support requirements. "You'll have to support two versions of Windows," he said. "Each needs to be secured, antivirused, firewalled and patched. If a company has 10,000 PCs, that's 20,000 instances of Windows."

Silver also noted that the add-on might lead companies to neglect the important task of making sure their applications are compatible with Windows 7. "This is a great Band-Aid, but companies need to heal their applications," he said. "They'll be doing themselves a disservice if, because of XPM, they're not making sure that all their apps support Windows 7."

Silver added that while Microsoft is effectively extending the life of Windows XP by offering it as a Windows 7 add-on, it hasn't changed its plan to shift the older operating system out of mainstream support and provide only what it calls "extended" support only until mid-April 2014.

"[XPM] will give some a false sense of security," Silver warned. "What happens in 2014, when XP isn't supported anymore? I think companies will be much better off if they make all their applications run on Windows 7."

— *Gregg Keizer*

Short Takes

The European Commission said that Microsoft Corp. has asked for an oral hearing to defend itself against antitrust charges that it is illegally tying its Internet browser to the Windows operating system. No hearing date has been set.

Qualcomm Inc. has agreed to pay chip designer Broadcom Corp. $891 million to settle a long-running patent dispute. The agreement ends litigation in the U.S., the EU and South Korea and gives each company the right to use the other's patent portfolio for four years.

Microsoft has started offering its hosted Exchange, SharePoint, Office Communications and Office Live Meeting services to companies in 18 countries outside of the U.S. where users had been limited to trial use.

The American National Standards Institute said it plans to develop a new specification for encrypting payment card data while it's in transit between systems during the transaction process.

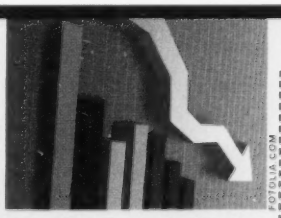
SERVERS

Sun Reports Its Sales Took A Big Hit in Last Quarter

SUN MICROSYSTEMS INC. last week reported another sharp drop in revenue for its fiscal third quarter, during which the company battled uncertainty about its future along with the global recession.

Reports that Sun was discussing an acquisition with IBM surfaced in mid-March, and the vendor eventually agreed to sell itself to Oracle Corp. two weeks ago. Analysts said the rumors could disrupt Sun's efforts to close deals late in the quarter that ended March 29, and that appears to have happened.

Sun said its Q3 revenue was $2.61 billion, down 20% year-to-year, resulting in a $201 million net loss. Sales of its x86 servers, which had been



a growth area, declined for the first time during the quarter. Total server shipments were off by 26% from last year's third quarter, according to Sun.

"There were few product categories that had any success this past quarter," said Gartner Inc. analyst George Weiss. "There will be a lot on Oracle's agenda to at least try to reverse the direction in some of them."

Sun has now posted losses in four of the past five quarters, and its revenue has declined in each of them. The company didn't hold a conference call on the third-quarter results, and its executives made no comments in the earnings report, presumably because of Oracle's pending acquisition.

– JAMES NICCOLAI, IDG NEWS SERVICE

CYBERSECURITY

Critics Argue Against a White House Security Lead

CRITICS RAISED questions last week about the growing chorus of calls for the White House to play a leading role in coordinating cybersecurity efforts involving the federal government and key private-sector industries.

Sen. Susan Collins

For instance, Sen. Susan Collins (R-Maine), the ranking Republican on the Senate Committee on Homeland Security, said at a hearing on cybersecurity strategies that putting the White House in charge would make it harder for Congress to oversee policies and budgets.

The president rightly should be responsible for "declaring [cyber] war," with input from Congress, Collins said. But for overall cybersecurity leadership, she suggested that the government use as a model the National Counterterrorism Center, which was set up in 2004. The NCTC is part of the Office of the Director of National Intelligence, a setup that allows Congress to play a role, Collins said.

Despite her concerns, a second bill that would give the White House more control over security efforts was introduced in the Senate last week. The measure proposed by Sen. Thomas Carper (D-Del.) would establish a National Office for Cyberspace whose director would be appointed by and report to the president.

A bill introduced early last month by Sens. Jay Rockefeller (D-W.Va.) and Olympia Snowe (R-Maine) would similarly create a cybersecurity office in the White House. In addition, Melissa Hathaway, a federal official who led a review of government cybersecurity programs, said two weeks ago at the RSA Conference that the White House should coordinate security efforts on a national basis.

But Stewart Baker, a former assistant secretary at the Department of Homeland Security, also argued against shifting control to the White House. Baker said the government should strengthen the ability of the DHS to manage cybersecurity by giving it the required resources as well as support from the National Security Agency and the military.

— Jaikumar Vijayan

BETWEEN THE LINES *By John Klossner*

BENCHMARKS LAST WEEK

President Barack Obama appointed Google Inc. CEO Eric Schmidt and Craig Mundie, who heads research at Microsoft Corp., to his council of science and technology advisers.

Google released the final version of a software developer's kit for Android 1.5, an update of the open-source mobile operating system.

10 YEARS AGO: The U.S. Department of Justice asked a federal judge to split Microsoft in two as part of the antitrust case against the vendor, which called the proposal "a regulatory death sentence."

Global Dispatches

EU Official Sees Need for Cyberchief

BRUSSELS – Viviane Reding, European Commissioner for Information Society and Media, last week called on the European Union to hire a top-level cybersecurity official to plan for and manage the EU's response to an attack on Internet infrastructure.

In a video blog posted last week, Reding accused EU member states of being "negligent" for failing to adequately prepare for the sort of attacks seen in Estonia, Lithuania and Georgia in recent years (see story, page 33).

Reding estimated that there is a 10% to 20% chance of an attack on the Internet infrastructure in the EU over the next 10 years. "A one-month-long Internet interruption in Europe would mean economic losses of at least €150 billion [$199 billion U.S.]," she said.

Paul Meller,
IDG News Service

Europe Awards OS Research Grant

AMSTERDAM – The European Research Council has awarded a €2.5 million ($3.3 million U.S.) grant to Vrije University to continue its work on Minix, a Unix-type operating system that aims to be more reliable and secure than Linux or Microsoft Windows.

The grant will fund three researchers and two programmers for five years, said Andrew Tanenbaum, a computer science professor at the Amsterdam school.

The latest grant will fund research into making the operating system capable of fixing itself when a bug is detected, Tanenbaum said.

Jeremy Kirk,
IDG News Service

BRIEFLY NOTED

Nokia Corp. last week announced plans to lay off 450 employees to further cut costs. The Espoo, Finland-based telecommunications company said the move, coupled with earlier layoffs of more than 2,000 workers, should cut costs by more than €700 million ($927 million U.S.) by 2010.

Mikael Ricknäs,
IDG News Service

Your old notebook can still be put to use. A new one from CDW can be put to work.

Lenovo ThinkPad® SL500

- Intel® Centrino® Processor Technology
  - Intel® Core™2 Duo Processor T5870 (2GHz)
  - Intel® Wireless WiFi Link 5100AGN
- Memory: 2GB
- 160GB hard drive
- DVD±RW drive
- 15.4" WXGA display
- Windows® XP Professional downgrade installed[1]

$778.99
CDW 1733386

Lenovo ThinkPad® R400

- Intel® Centrino® 2 Processor Technology
  - Intel® Core™2 Duo Processor P8400 (2.26GHz)
  - Intel® Wireless WiFi Link 5100AGN
- Memory: 2GB
- 160GB hard drive
- DVD±RW drive
- 14.1" WXGA display
- Windows® XP Professional downgrade installed[1]

$998.99
CDW 1524888

Lenovo ThinkPad® T500

- Intel® Centrino® 2 Processor Technology
  - Intel® Core™2 Duo Processor P8400 (2.26GHz)
  - Intel® Wireless WiFi Link 5100AGN
- Memory: 2GB
- 160GB hard drive
- DVD±RW drive
- 15.4" WXGA display
- Windows® XP Professional downgrade installed[1]

$1148.99
CDW 1524904

We're there with the technology solutions you need.

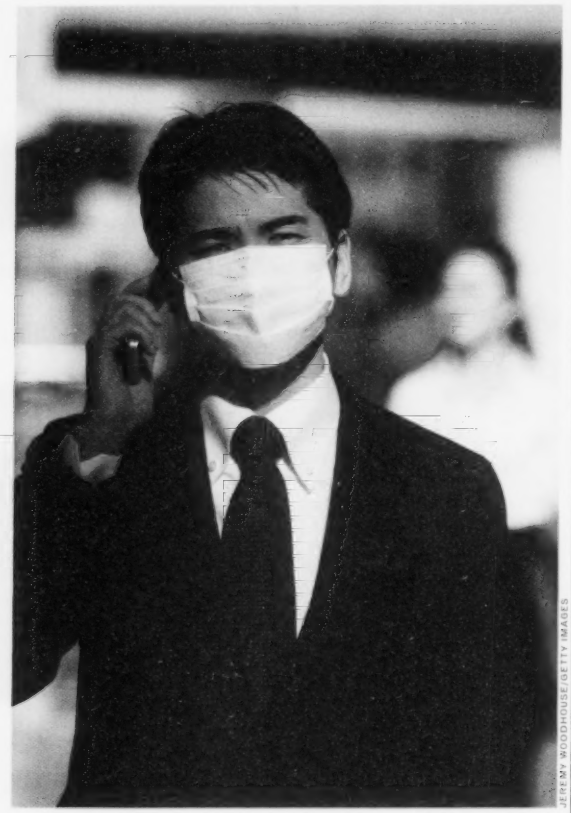
Sure, outdated technology can serve your needs. But unfortunately, not your work needs. When you upgrade to new technology from CDW, you'll be more productive than ever. If you need to go mobile, you can with countless wireless options. Need to upgrade to a new operating system? No problem. Of course, we also offer a personal account manager who knows the needs of your business, as well as a host of configuration services. Bottom line – we'll make sure you get what you need, when you need it. So call CDW today and work smarter, not harder.

CDW.com | 800.399.4CDW

CDW

The Right Technology. Right Away.™

[1]Windows® XP installed with Windows Vista® Certificate of Authenticity and logo. Windows Vista media included. Customer has rights to both Windows Vista and Windows XP Professional. Offer subject to CDW's standard terms and conditions of sale, available at CDW.com. ©2009 CDW Corporation



JEREMY WOODHOUSE/GETTY IMAGES

IT Faces Possible Pandemic Amid Budget Cutbacks

Analysts suggest that managers update IT call lists and telecommuting plans. By Patrick Thibodeau

MANY IT executives could be facing an uphill battle in moving to deal with a possible swine flu pandemic as they cope with a flagging economy that has caused layoffs and budget cutbacks in a number of companies.

Jim Grogan, vice president of consulting product development at SunGard Availability Services LP in Wayne, Pa., recommended last week that IT managers immediately review call lists and decision-making chains that may include victims of downsizing or other cost-cutting measures.

"There could be a weakness in plans because of organizational restructuring that people need to very quickly take a look at," he said.

Grogan also suggested that organizations that can't create a specific pandemic plan turn to any procedure created to deal with a "significant absence" of employees. The standard model used in pandemic planning is to consider what would happen to a business if 40% of the workforce was absent for an extended period of time, he noted.

The World Health Organization (WHO) late last week raised the swine flu alert level to Phase 6 on a scale of 1 to 6, indicating a "widespread human infection."

By last Wednesday, the Centers for Disease Control and Prevention (CDC) in Atlanta had reported one death in Texas among 91 cases of swine flu in the U.S., including 50 in New York, 26 in Texas, 14 in California and 10 in South Carolina. In a statement on its Web site, the CDC added that "more hospitalizations and more deaths are expected in the coming days and weeks." At the same time, the WHO reported 8 deaths among 257 cases of swine flu worldwide.

In a *Computerworld* blog post early last week, Scott McPherson, CIO of the Florida House of Representatives, advised data center executives to begin "reviewing your pandemic plans now, and familiarizing yourself with them again immediately. It is probably too late to buy anything, or to buy anything more. So all we can do is educate our people (quickly!), plan, and watch."

"I think we are well prepared — I think a lot of sectors are better prepared than they were a few years ago," said Shawn Johnson, a senior managing director at State Street Global Advisors Inc. in Boston. Johnson is also chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, a security trade group formed in 2002.

Gartner Inc. analyst Rick DeLotto said he is advising clients to check their telecommuting capabilities and make sure that assistant managers can take over if necessary. If absenteeism rises because the flu spreads, "there are going to be a lot of very rapidly promoted assistant managers who have to have the right permissions and provisioning," he said.

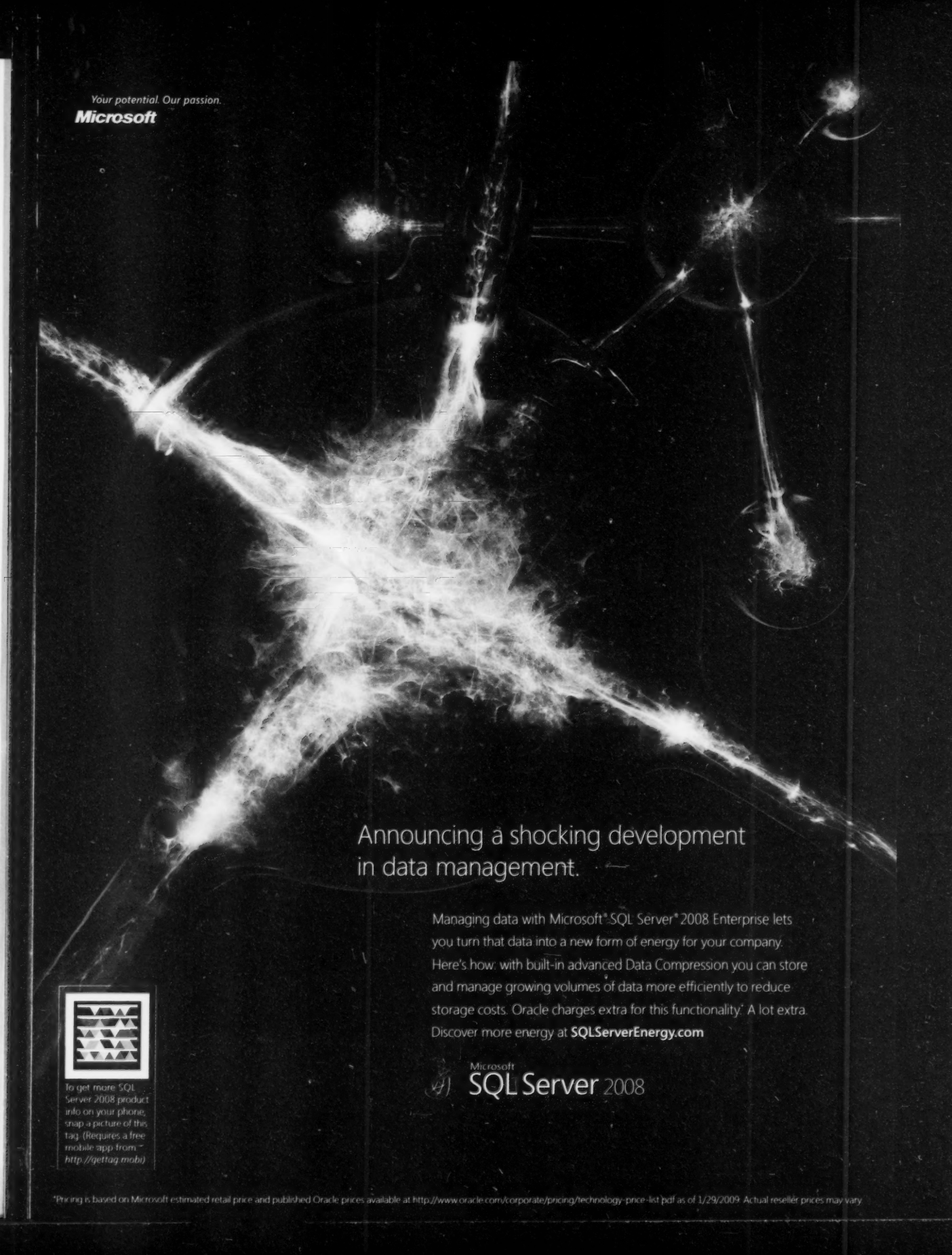
In addition to letting employees know that they are responding to this threat, companies need to urge workers to wash their hands, as well as make face masks available for them, DeLotto said.

After the WHO raised the threat level last week, Gartner analyst Ken McGee issued an advisory calling on companies to begin preparing workers for widespread telecommuting and videoconferencing, and setting up options for dealing with network outages, among other things.

Meanwhile, several Japan-based electronics companies had halted business trips to Mexico by early last week.

Panasonic Corp. and Sharp Corp., both based in Osaka, halted all business trips to Mexico City, while Tokyo-based Sony Corp. asked employees to avoid travel to the Mexican capital. ■

Martyn Williams of the IDG News Service contributed to this story.


Your potential. Our passion.
Microsoft
Announcing a shocking development in data management.
Managing data with Microsoft® SQL Server® 2008 Enterprise lets you turn that data into a new form of energy for your company. Here's how: with built-in advanced Data Compression you can store and manage growing volumes of data more efficiently to reduce storage costs. Oracle charges extra for this functionality.* A lot extra. Discover more energy at SQLServerEnergy.com
Microsoft SQL Server 2008
To get more SQL Server 2008 product info on your phone, snap a picture of this tag. (Requires a free mobile app from http://gettag.mobi)
*Pricing is based on Microsoft estimated retail price and published Oracle prices available at http://www.oracle.com/corporate/pricing/technology-price-list.pdf as of 1/29/2009. Actual reseller prices may vary.

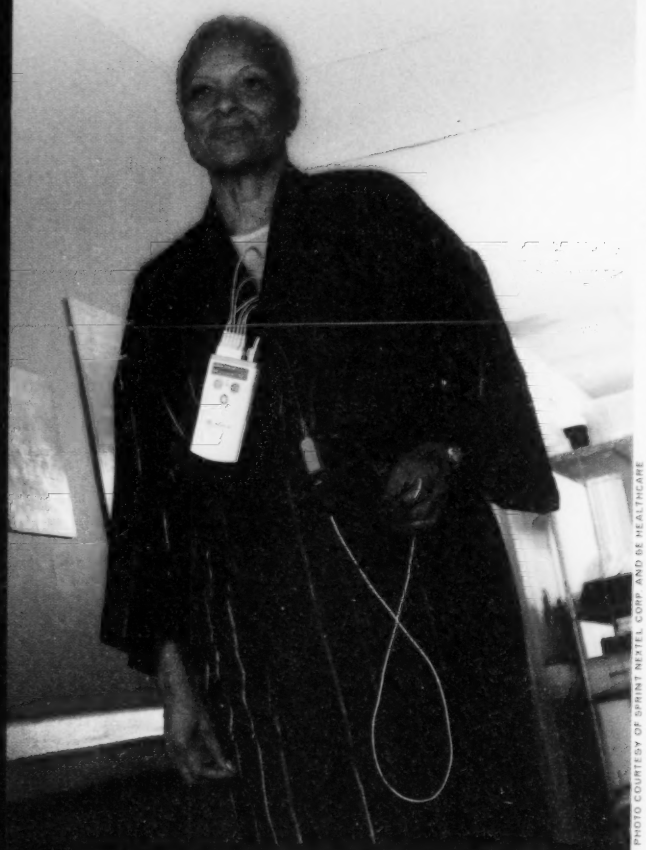


PHOTO COURTESY OF SPRINT NEXTEL CORP. AND GE HEALTHCARE

GE Healthcare's Carescape telemetry system uses a wireless transmitter to send vital-signs data to a central server.

Wireless IT in Health Care: The Time Is Now?

Wireless medical apps are ready for broad usage and could transform patient care. That's what proponents say, at least. **By Matt Hamblen**

AFTER YEARS of talk about wireless technologies' potential for widespread use in medical applications, they appear to be ready for a takeoff in adoption within health care organizations.

And some doctors and IT professionals think that wireless has the potential to transform health care in the U.S. by improving patient care and lowering costs.

It remains to be seen whether that will prove to be a sound prediction or yet another case of cockeyed optimism about new technologies. But wireless proponents such as Dr. Eric Topol are in a bullish mood.

Topol, a cardiologist and administrator at Scripps Health in San Diego, is a longtime advocate of wireless technologies and has worked as an adviser and board member at some start-ups. In a keynote speech at last month's International CTIA Wireless 2009 conference in Las Vegas, he pointed to a number of technologies that are either on the market or being used in trials, claiming that they could help improve patient monitoring and reduce errors in administering medications.

"At the same time the economy has hit bottom, we've never had more exciting innovation in wireless medicine," said Topol, who is chief academic officer at Scripps Health and director of the Scripps Translational Science Institute, a research unit.

In an interview, Topol cited three reasons for the increasing interest in wireless technologies: bandwidth improvements that enable the transmission of images and other rich medical data, an influx of applications from software vendors, and what he called the "grand success" of recent efforts to improve the quality of patient care through wireless projects.

Topol said that over the past two years, he has seen a huge improvement in the personalization of care for his own patients through the use of wireless cardiac-monitoring tools. Sensors attached to a patient's chest can transmit real-time metrics such as heart rhythms, body temperature and blood-oxygen levels, enabling Topol to look at weeks of information when making a diagnosis and devising a treatment plan.

In the past, just two or three days' worth of heart data was typically recorded for each patient, he said, adding that the new technologies provide "a much broader window of the heart rhythm to watch."

During his CTIA keynote, Topol demonstrated several technologies, including an adhesive heart sensor developed by Corventis Inc. that he had placed on his chest. The patch transmitted a variety of data to a monitor that displayed the information as a doctor or medical technician would see it, including a diagram of Topol's body position to show whether he was standing or lying down.

Corventis announced the availability of its "wearable sensors" on April 21. Other wireless cardiac-monitoring vendors include LifeWatch Corp. and CardioNet Inc., where Topol once served on the medical advisory board. (He is currently a member of the board of directors at Triage Wireless

PHOTOGRAPH COURTESY OF CARDIONET

CardioNet's wireless heart monitor receives data from a sensor attached to a patient.

Inc., a start-up that is testing a wireless application for monitoring blood pressure and other vital signs.)

Brent Atwood, LifeWatch's chief operating officer, said the use of the company's LifeStar ACT technology has grown from 35,000 patients in January 2007 to about 120,000 now. The technology transmits heart rhythm data via a Bluetooth connection to a cell phone equipped with a specialized interface. For periods of up to 21 days, the phone continuously sends the data to a LifeWatch call center, where software detects any irregularities and alerts cardiac technicians.

LifeWatch is moving all of its cellular connections to the Verizon Wireless network and plans to work with the mobile carrier to expand its support to wireless monitoring of conditions such as diabetes and sleep disorders, Atwood said.

Methodist Healthcare System, which operates 23 medical facilities in the San Antonio area, is implementing a wireless patient-monitoring and communications system at six hospitals. The multimillion-dollar project was jointly announced by Sprint Nextel Corp. and General Electric Co.'s GE Healthcare unit on April 6.

The new system will use GE's Carescape technology and the dedicated Wireless Medical Telemetry Service frequency to transmit patient data to medical personnel equipped with more than 800 Sprint Nextel phones.

PRODUCTIVITY BOOST

"There's a lot of pressure in health care to become more efficient, and it's made worse by the shortage of nurses," said Eddie Cuellar, Methodist's CIO. "We have to find a way to make them more productive as they walk back and forth on hallways 20 to 30 times a day."

One of the wireless applications being rolled out by the health care system is AirStrip Technologies LP's AirStrip OB, which will send fetal monitoring data to obstetricians. That should enable doctors to move more freely between patients, both within one hospital and at different facilities, while still keeping track of how each patient's labor is progressing, Cuellar said.

Intermountain Healthcare in Salt Lake City runs patient monitoring applications at 23 medical facilities over a Wi-Fi network that's based on technology from Cisco Systems Inc. The network, which cost about $3 million to set up, is now also being used to transmit data from infusion pumps, the portable devices used to administer medications intravenously, said Ty Bindrup, an enterprise network planner at Intermountain.

As the data is sent from the pumps to messaging and alarm-management middleware from Emergin Inc., "we can see how much of a drug a patient has received," Bindrup said. The information can then be compared against appropriate-dosage data in an effort to lower the chances of errors, he added.

Not everyone is convinced, though, that wireless applications will sweep through the health care industry and remake medical practices in the process.

For example, Gartner Inc. analyst Wes Rischel thinks wireless technologies clearly hold promise for health care, but he said IT managers and hospital officials shouldn't get carried away with optimism about the tools. Rischel pointed to RFID technology as a cautionary tale, saying it has been pushed in the health care market for more than 10 years but isn't well suited to tracking medical equipment. "There's plenty of hype there, but not much acceptance," he noted.

The wireless networks used in hospitals and the applications offered by vendors have matured over the past two years, Rischel said, adding that he does expect "accelerating growth" in adoption.

Even so, he characterized technologies such as the heart-sensor patch that Topol demonstrated at CTIA as "incremental advances." The real revolution in health care IT, Rischel said, will likely come from something else: increased deployments of electronic medical records systems and the resulting improvements in data-sharing among organizations. ■

Medical Lab Stems Losses Via Wireless Tracking App

Pathology Associates Medical Laboratories has become a big believer in wireless technology.

PAML provides lab services to more than 100 hospitals in the northwestern U.S., testing about 60,000 medical specimens annually. But it had a problem: a relatively high rate of lost specimens.

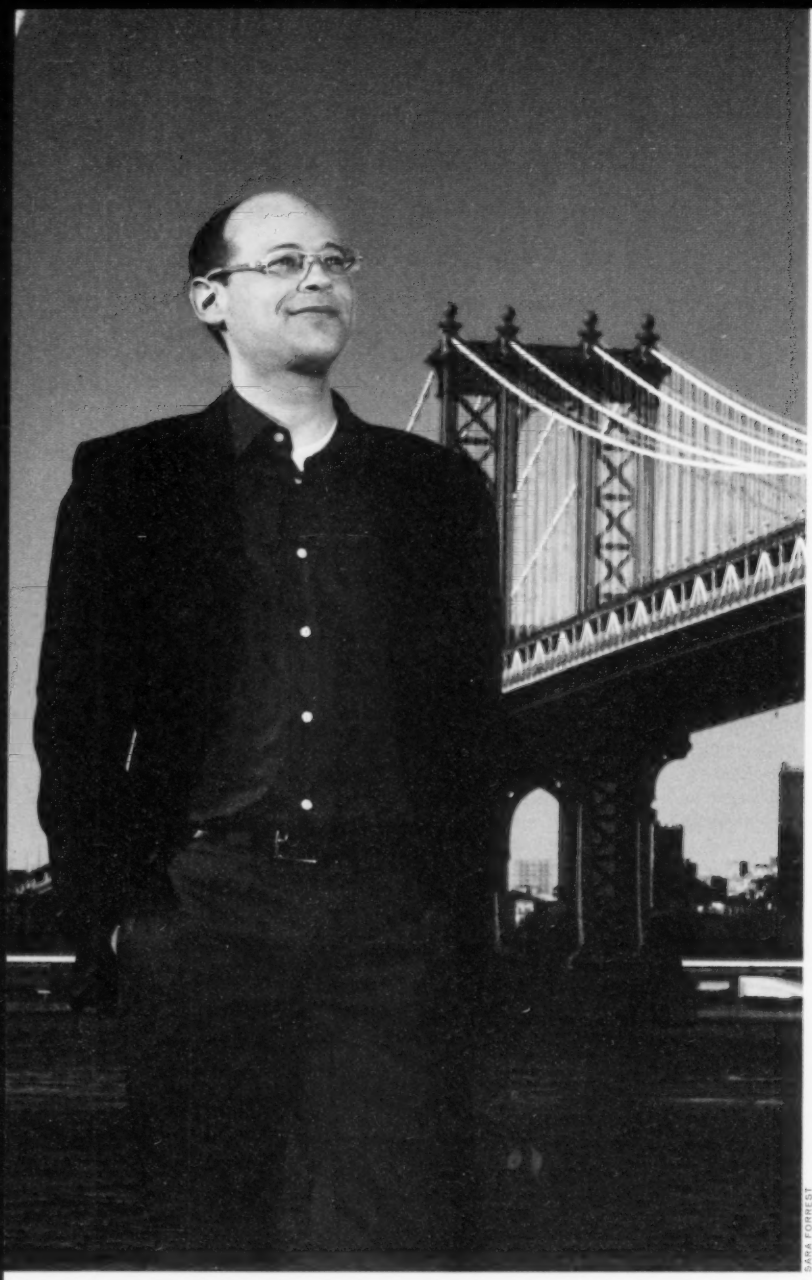
Now the Spokane, Wash.-based lab's tracking ability has improved dramatically through the use of a wireless communications and bar code system, according to Rosalee Allan, its chief operations officer.

The two-year-old system, which replaced a paper-based process, uses software from Dexterra Inc. and ruggedized Motorola MC70 handheld devices that run Windows Mobile and communicate via AT&T Inc.'s wireless network.

PAML's 200 couriers use the MC70 devices to read bar codes affixed to medical specimens, and the wireless technology is integrated with the lab's CRM system based on Microsoft Corp.'s Dynamics applications. That enables PAML to keep track of specimens in much the same way that FedEx and UPS monitor packages, Allan said.

"Wireless totally changed our reputation," she added. "Previously, we were known for losing specimens, and we had no tracking system." With the new system, she said, fewer than three of every 100,000 specimens are lost, which is "much better than it was" before.

– MATT HAMBLEN



SARA FORREST

Dossier

Name: Robert Faludi

Title: Adjunct professor

Organization: New York University

Location: Manhattan

Most interesting technology: "The world is full of gadgets, but what I'm really impressed with is tomato seeds. Press one seed into wet soil, and up pops a contraption that turns sunlight into food. It's humbling."

Philosophy in a nutshell: "Technology succeeds when it lets humans be more human."

People he most admires: "The Inuit, for respecting their environment while pressing the boundaries of survival."

Favorite New York restaurant: Jimmy's No. 43

Favorite plant: Lithops, the "living stone"

■ THE GRILL

Rob Faludi

The **networking visionary** talks about introducing your **toaster** to your **smoke alarm,** bonding with your **plants** and bringing the **outside** in.

Rob Faludi is a specialist in physical computing and networked objects. As a researcher in New York University's psychology department and Center for Neural Science, he has investigated the connections between visual perception, motor action and the physical environment.

You had your own company for 10 years in San Francisco. Why did you move back to New York and go into teaching? Couldn't get a decent slice of pizza. And I really missed winter. Mostly, though, I came back to New York to better understand people. My consulting company had been doing some cutting-edge work. In team meetings, we'd get embroiled in lengthy debates about how [a Web] interaction should proceed. When we finally put our creations in front of real users, they'd frequently breeze through the parts that we thought would be hard and then screech to a halt, completely bewildered by some choice that everyone on the development team had assumed would be obvious. I wanted to know what was going on. The answers would span science and design, so I returned to school for two master's degrees, one in cognitive psychology and one from NYU's Interactive Telecommunications Program. When it was all

Continued on page 20

verizon wireless

Questions about mobile email?

Tracking shipments?

What that green button does?

Dedicated Small Business Specialists are in every Verizon Wireless store, all at no extra charge.

Our experts will:

- Help you choose the right mobile email solutions.
- Show you how to use business technology to your advantage.
- Have you up and running before you leave the store.

BlackBerry Storm™ $199.99
With 2-yr activation on voice plan with email feature or email plan.

Buy ANY BlackBerry® and get any other BlackBerry® FREE

Free BlackBerry Smartphone of equal or lesser value. New 2-yr activation on voice plan with email feature, or email plan req'd per phone.

One of the many tools in the **Verizon Wireless Small Business Toolbox.**

Call 1.800.VZW.4BIZ Click verizonwireless.com/smallbusiness Visit your local Verizon Wireless store

Activation fee/line: $35.
IMPORTANT CONSUMER INFORMATION: Subject to your Major Account Agreement or Customer Agreement, Calling Plan, rebate form and credit approval. Up to $175 early termination fee/line and other charges. Device capabilities: Add'l charges apply. Offers and coverage, varying by service, not available everywhere. Network details and coverage maps at verizonwireless.com. While supplies last. Shipping charges may apply. Limited-time offer. ©2009 Verizon Wireless.

"When that phone call or text message comes in from your plant, we're hoping to precipitate a moment that you and your leafy friend can spend together.

Continued from page 18

done, ITP asked me to do some teaching. That's turned out to be a terrific way to keep on learning.

Can you define "sociable objects" and describe how you became interested in creating them? Sociable objects are simply devices that share information with each other and with people. The well-socialized object knows when and how to share. It doesn't bother you with questions it could answer on its own. It's happy to socialize with the other devices nearby, requesting information and lending a hand when it can.

When I push [my toaster] lever down, if there's a crumb stuck in the coils, it isn't long before my fragile pre-coffee state is shattered by the piercing siren of my smoke detector. It doesn't know about the toast, but really it should. If it were sociable, as soon as it detected particulate matter in the air, it would query the toaster to see if it had been activated. That would tell it that in all likelihood, it wasn't detecting an unattended, middle-of-the-night fire but instead a benign morning meal. The price of low-power radio networking and the just-minted funding for smart home energy networks makes this sociable smoke-detector scenario entirely within our reach. I want one.

Do your studies in psychology and neural science help you facilitate different ways of human-object communication? Oh, it's all about the people for me! I deeply respect engineering and computer science because they are fundamentally human endeavors. What I aim to do is take the magic they produce to the next level and find ways that new technologies can engage us and enrich our interactions.

Can you briefly touch on the concept of mesh networking? Broadly speaking, a mesh network is a collection of devices that are all connected to each other both directly and indirectly. Any one device can act as both a node and a router for other nodes. Together, the devices create a robust communications structure, one that adapts fluidly when a new device enters the network or another one is removed or fails. There are over a hundred ad hoc routing protocols for these networks, but the basic idea is a kind of egalitarian structure. It's terrific for making robust and highly flexible local networks — kind of like a party where everyone is making introductions to everyone else and happily chatting away, changing their layout as people enter and leave the room. On the other hand, it's an inappropriate structure for very large networks because the overhead of routing everything to everyone rapidly becomes unmanageable. So usually network architects use mesh at a local level and then route to a more hierarchical topology for internetworking. That way, the local fetes can stay fun without devolving into a shouting match.

Can that type of networking be applied to solving current environmental problems? I've been developing networks for home energy monitoring with a start-up called GroundedPower Inc. We're rolling out a pilot project for Cape Light Compact, an energy services organization responsible for efficient and environmentally responsible power on Cape Cod and Martha's Vineyard. We're creating a way for their customers to see exactly how much energy they're using in real time. The pilot project will look at how and to what extent consumers respond to real-time information about electricity consumption and how their conservation actions are affected by being part of a community network. This is a great example of how objects and networks can have a real impact on not just individuals' lives, but on the way we impact the world as a whole. If we can get enough people monitoring their power consumption and leverage that effectively into behavior change, then perhaps we can keep the oceans where they are. I like sushi, but I don't want to live with it.

You also co-created a human-plant communication system. How does it work? The Botanicalls project aims to forge a connection between people and nature. Botanicalls is about helping people notice the other living things around them. When that phone call or text message comes in from your plant, we're hoping to precipitate a moment that you and your leafy friend can spend together. So the technology of sensing soil moisture, connecting to an online message generator and triggering notifications is really about momentarily fracturing the grip of gadgets and nudging a person back toward the tiny bit of wild that shares their space.

And that brings up Wild Light. Tell me about that. Wild Light springs from the same conceptual source as Botanicalls, and it's a very straightforward system. The idea is to bring the rhythms of organic daylight into dark and windowless spaces. In urban and office environments, we frequently cut ourselves off from the reality of the day so much that when finally venturing outside, we're shocked to discover bright sunshine or maybe torrential storms. The basic Wild Light setup is simply a lamp with a networked connection to an outdoor solar sensor. This allows the indoor fixture to directly reproduce real-time natural lighting, on a scale where if a cloud flits across the sun, your Wild Light lamp will momentarily dim and brighten. It's harnessing technology to reconnect us to nature's capriciousness. I think those exposures are good for the soul.

— Interview by **Sara Forrest,** *a freelance photographer and writer in New York (saraforrestphoto@gmail.com)*

IT Innovations Forum

Thursday, May 7, 2009

Live Interactive Online Conference

http://virtualconferences.computerworld.com/itinnovations

Register today, it's free.

Learn to Thrive in Turbulent Times

Get real-world answers and customer-proven solutions you can implement immediately from your industry peers, independent analysts, and technology experts at this in-depth, interactive conference. Exchange ideas and gain valuable insights in real time from panelists as well as your fellow attendees. See the latest innovations at virtual product booths from the convenience of your desktop and learn how they can simplify your IT workload and reduce your operating expenses.

8:00am Eastern Daylight Time (New York)
12:00pm Greenwich Mean Time
1:00pm British Summer Time (London)
5:30pm Indian Standard Time

*All sessions available on-demand following initial broadcast

Follow Cisco for more updates on Facebook and Twitter.

facebook twitter

CISCO COMPUTERWORLD InfoWorld

SPECIAL REPORT

INTERNET WARFARE:
Software: The Eternal

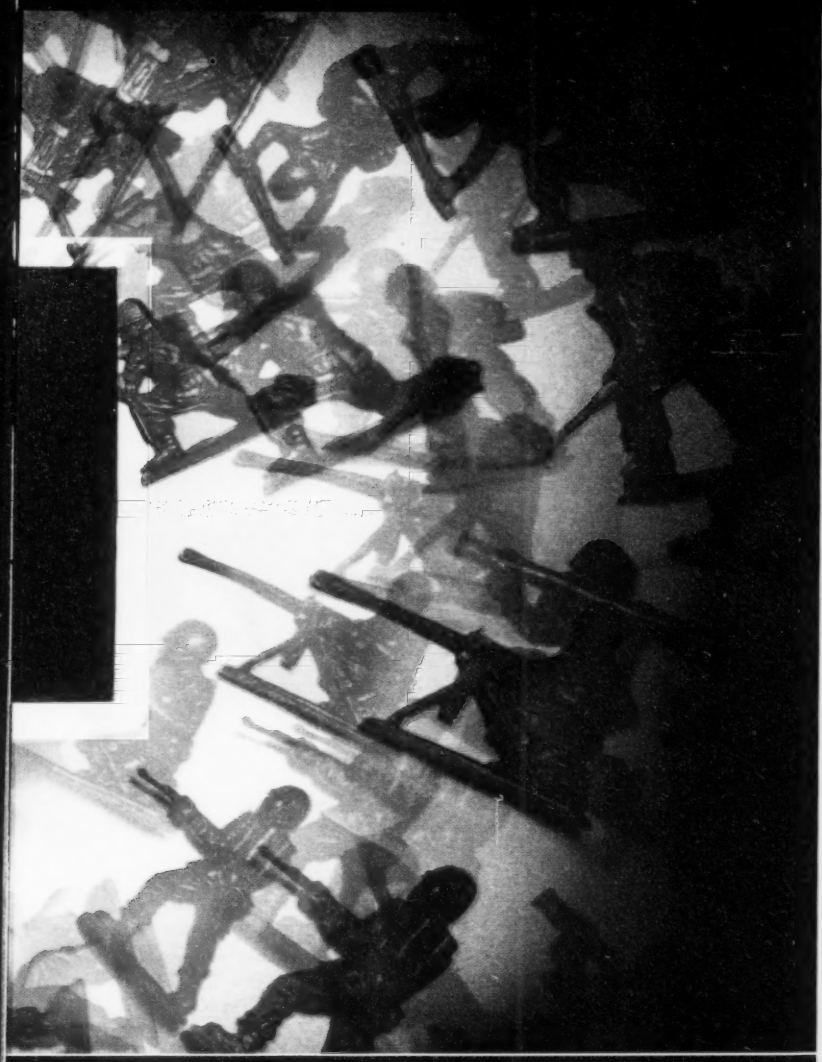
We are at risk. Computers are vulnerable to the effects of poor design, insufficient quality control, accident and, perhaps more alarmingly, to deliberate attack.
– *Computers at Risk*, Computer Science and Telecommunications Board, National Research Council, 1991

Eighteen years later, we are still at risk. Our computers are still vulnerable. They still suffer attacks enabled by poor design and insufficient quality control. We spend huge sums on IT security, yet U.S. companies and individuals are losing tens of billions of dollars annually to cybercrime.

In January, Heartland Payment Systems Inc. reported what may be the largest data heist ever.

The company said that a "global cyberfraud operation" stole information from more than 100 million credit card holders. Someone had planted a software "sniffer" in a Heartland serv-

ILLUSTRATION: ANASTASIA VASILAKIS



Internet attacks take many forms, but most of them exploit persistent software weaknesses. By Gary Anthes

Battlefield

er, where it apparently nosed around undetected for weeks.

Those kinds of megabreaches make big news and cause their victims big pain. But they are just the tip of a huge iceberg. Last September, Gartner Inc. published a chilling case study about The Procter & Gamble Co., a business known for its IT sophistication and one with a robust deployment of firewalls and intrusion-detection and antivirus tools. P&G conducted a six-month worldwide audit of its PCs to see if any were infected by hidden software robots, or bots, which can connect to botnets secretly controlled by external parties.

Using special sensor software, P&G discovered that some 3,000 of its 80,000 PCs were infected with botnet clients. Those bots were attempting to communicate with a dozen remote sites, with about 20% of those attempts getting through P&G security systems.

But that's not all. P&G scrubbed the offending bots by reimaging the PCs, a laborious process of removing and reinstalling all the software, including the operating system. According to Gartner, however, many PCs became reinfected immediately when backed-up user data that contained hidden executables was restored to the reimaged machines.

In the past 18 years, there have been amazing advancements in every facet of IT — in networks, processors, memory, disks, languages, applications, development methods and security tools. Yet technology clearly has not turned the tide of war with cybercriminals.

"Our opponents in cybersecurity are winning, and they will continue to win," says Jim Routh, chief information security officer at The Depository Trust & Clearing Corp. in New York. "This is not a war we will ever see an end to."

William Scherlis, a professor of computer science at Carnegie Mellon University and a specialist in software security and reliability, says that attacks today are more sophisticated and more stealthy and are carried out much faster than ever before. He points to three trends in IT that are making the problem worse. "They are obvious, but they have crept up on us, and the world is now radically different," he says.

The first is a pervasive shift away from functional system silos to interconnected, enterprise and cross-enterprise systems. A failure at one spot can influence or cascade to places far removed in time, geography and function.

The second is a decentralization of IT responsibility, with some of it going to non-IT people. "One change — such as a simple change in access privileges by an administrator or a change to a business rule by a marketing expert — can ripple across a worldwide enterprise," Scherlis says.

The third factor, related to the other two, is the extreme speed with which actions — simple mistakes as well as at-

SPECIAL REPORT

INTERNET WARFARE:

Software: The Eternal

"We are at risk. Computers are vulnerable to the effects of poor design, insufficient quality control, accident and, perhaps more alarmingly, to deliberate attack.
– *Computers at Risk*, Computer Science and Telecommunications Board, National Research Council, 1991

Eighteen years later, we are still at risk. Our computers are still vulnerable. They still suffer attacks enabled by poor design and insufficient quality control. We spend huge sums on IT security, yet U.S. companies and individuals are losing tens of billions of dollars annually to cybercrime.

In January, Heartland Payment Systems Inc. reported what may be the largest data heist ever.

The company said that a "global cyberfraud operation" stole information from more than 100 million credit card holders. Someone had planted a software "sniffer" in a Heartland serv-

ILLUSTRATION: ANASTASIA VASILAKIS

Internet attacks take many forms, but most of them exploit persistent software weaknesses. By Gary Anthes

Battlefield

er, where it apparently nosed around undetected for weeks.

Those kinds of megabreaches make big news and cause their victims big pain. But they are just the tip of a huge iceberg. Last September, Gartner Inc. published a chilling case study about The Procter & Gamble Co., a business known for its IT sophistication and one with a robust deployment of firewalls and intrusion-detection and antivirus tools. P&G conducted a six-month worldwide audit of its PCs to see if any were infected by hidden software robots, or bots, which can connect to botnets secretly controlled by external parties.

Using special sensor software, P&G discovered that some 3,000 of its 80,000 PCs were infected with botnet clients. Those bots were attempting to communicate with a dozen remote sites, with about 20% of those attempts getting through P&G security systems.

But that's not all. P&G scrubbed the offending bots by reimaging the PCs, a laborious process of removing and reinstalling all the software, including the operating system. According to Gartner, however, many PCs became reinfected immediately when backed-up user data that contained hidden executables was restored to the reimaged machines.

In the past 18 years, there have been amazing advancements in every facet of IT — in networks, processors, memory, disks, languages, applications, development methods and security tools. Yet technology clearly has not turned the tide of war with cybercriminals.

"Our opponents in cybersecurity are winning, and they will continue to win," says Jim Routh, chief information security officer at The Depository Trust & Clearing Corp. in New York. "This is not a war we will ever see an end to."

William Scherlis, a professor of computer science at Carnegie Mellon University and a specialist in software security and reliability, says that attacks today are more sophisticated and more stealthy and are carried out much faster than ever before. He points to three trends in IT that are making the problem worse. "They are obvious, but they have crept up on us, and the world is now radically different," he says.

The first is a pervasive shift away from functional system silos to interconnected, enterprise and cross-enterprise systems. A failure at one spot can influence or cascade to places far removed in time, geography and function.

The second is a decentralization of IT responsibility, with some of it going to non-IT people. "One change — such as a simple change in access privileges by an administrator or a change to a business rule by a marketing expert — can ripple across a worldwide enterprise," Scherlis says.

The third factor, related to the other two, is the extreme speed with which actions — simple mistakes as well as at-

■ SPECIAL REPORT

PORTRAIT OF A SECURITY-SAVVY USER

The Depository Trust & Clearing Corp. takes information security seriously.

It had better. The organization, which provides clearing, settlement and information services for financial institutions and government, settled $1.88 quadrillion (thousand-trillion) in securities transactions last year.

The DTCC claims to be the only financial services firm rated at Level 3 on the Software Engineering Institute's Capability Maturity Model Integration scale. It is also one of the co-developers of the just-announced industry-standard Building Security in Maturity Model.

"We have a very disciplined, process-oriented approach," says Jim Routh, the DTCC's chief information security officer.

Here's what the DTCC does:

- It subjects its internally developed software to the rigors of static and dynamic code analysis.
- It has its systems undergo penetration testing.
- It subscribes to a third-party service that scans its Web sites looking for vulnerabilities.
- It assigns risk levels – high, medium or low – to any vulnerabilities found.
- It remediates vulnerabilities and tracks remediation at three levels in the organization.

As for software vendors, the DTCC "puts them through the paces," Routh says.

For software deemed to be high risk, the vendors must show evidence of the same kinds of controls that the DTCC uses internally. "They have to show us the artifacts of their software development life cycle as it relates to security – static code analysis, dynamic analysis, penetration testing, and how they track vulnerabilities and manage their remediation," he says, adding that the DTCC is one of the few firms that does that.

Vendors that can't produce these artifacts get another chance, however. They must submit the software in question, in binary form, to an external party that scans it for high-risk vulnerabilities and assigns a grade to it.

"We pay for some of that," Routh says. "We get the high-level results, the vendor gets the detailed results, and we negotiate remediation priorities."

– GARY ANTHES

tacks — are propagated throughout networks and systems. "All three of these changes contribute value and agility to the enterprise, but they also reshape the security picture," Scherlis says.

A few years ago, an organization would have put an "enterprise firewall" between its internal systems and external networks, he explains. If it subsequently detected bad actors or bad software inside the company, it would have then turned to departmental firewalls and, soon after that, to firewalls on individual computers. Then, if that proved insufficient, the company would have started putting shields around individual applications.

Now, Scherlis says, even that is not enough, as systems become more and more fragmented yet interconnected. "Modern applications contain frameworks and libraries from diverse sources, and they stretch across multiple computers," he says. "So now you need to consider perimeters inside the application, at the application programming interfaces."

Even the simplest applications may contain thousands of individual executable components from multiple sources. "That makes the software assurance problem really hard," Scherlis says.

TURN THE TABLES

Fred Schneider, a software security and reliability expert at Cornell University, goes even further, saying that the notion of building defensive perimeters — at any level — is outdated.

"Today, people discover vulnerabilities because someone uses one in an attack, and then they fix it. They are walking around finding holes in the dike and patching them. This is playing catch-up and letting the attacker define the problem. It's an inherently losing mind-set."

But, Schneider suggests, "what if we turned the tables in a way that allowed us to stay ahead of attacks?"

Many Internet-borne attacks come via spoofing; you get a message purporting to be from, say, Citibank, but it's not, and it contains some malware. "Suppose every message on the Internet could be attributed to the person who sent it?" he says. "Then, when someone launched an attack, you could find out who sent it and arrest them."

Schneider says this would change the mind-set from one of prevention to one of accountability. People would behave, not because their misbehavior would be blocked, but because they could be caught and held accountable.

"The problem with the current prevention mentality is you have to protect everything," Schneider says, "but the attacker only has to find one chink in the armor."

Although not trivial, implementing such accountability on the Internet is technically feasible. But there are two big barriers to making it happen, Schneider acknowledges.

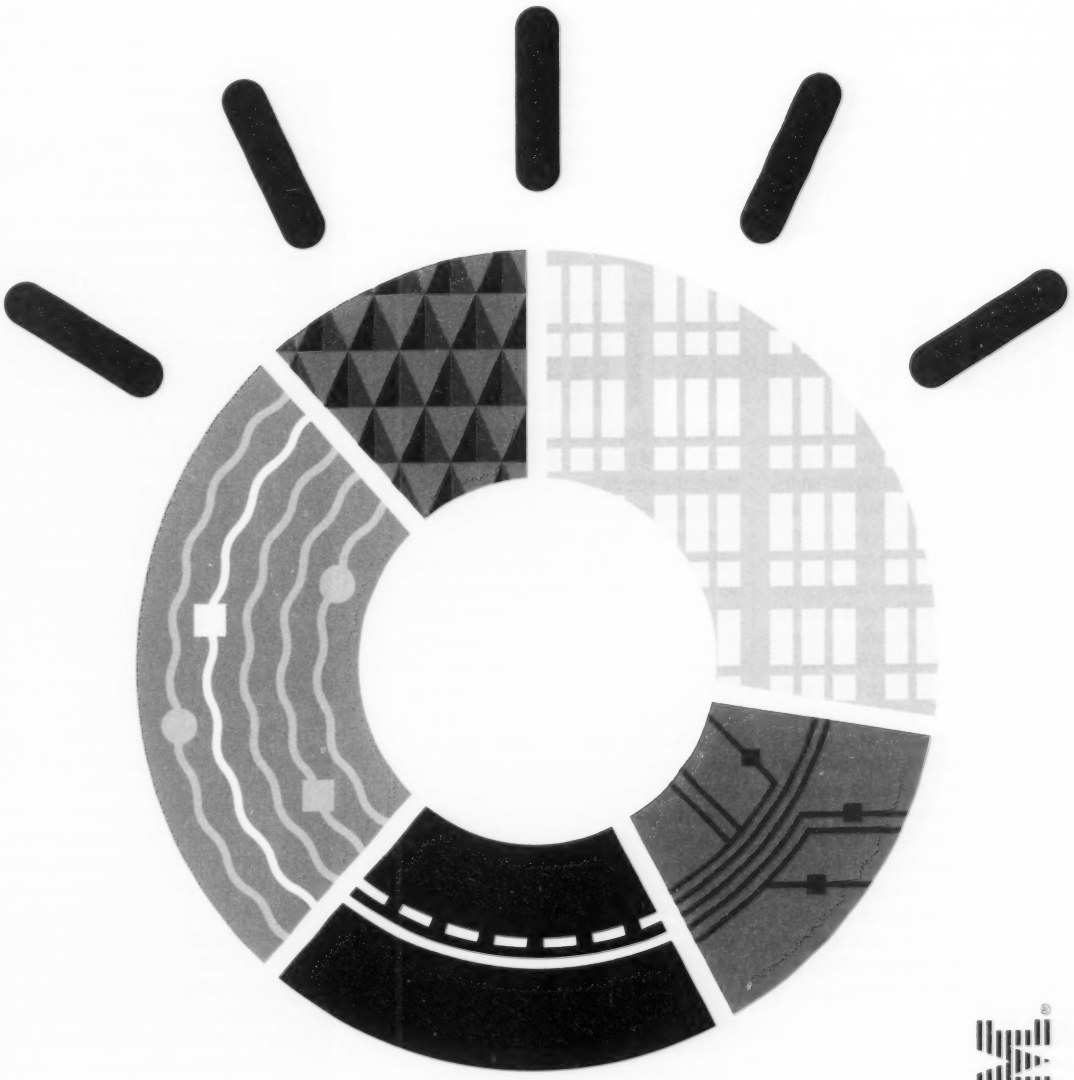
One is an expectation of anonymity that many users would not lightly relinquish. The other is that vagaries of local law and custom could render attackers outside the U.S. difficult to bring to account. "We need to strike a balance between accountability and anonymity," Schneider says, "and we

Continued on page 26

"Be absolutely rigorous about configuration management and configuration integrity, both during development and ceaselessly during operations.

WILLIAM SCHERLIS, PROFESSOR OF COMPUTER SCIENCE, CARNEGIE MELLON UNIVERSITY

Up to 85% of computing
capacity sits idle in
distributed environments.
A smarter planet needs
smarter infrastructure.
Let's build a smarter planet.
ibm.com/dynamic



THINK

IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.
A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Continued from page 24

need international agreements."

At least one major software maker may have gotten the message. In a paper published last year, Microsoft Corp. Vice President Scott Charney outlined steps the company has taken since 2002, when Bill Gates launched the Trustworthy Computing initiative that Charney now heads. Charney noted that the company has made progress in strengthening its products against attack, but he acknowledged that improving any given piece of software isn't enough.

Charney argues that we must fundamentally "change the game," and two things are needed to do that. The first is to build a "trusted stack," with strong authentication at every layer — hardware, software, people and data — something Microsoft calls end-to-end trust. The second is to implement Schneider's prescription for auditability of events to provide accountability.

So it seems users are in a holding pattern. They're waiting for software vendors to fortify individual products, something they've been doing slowly for years; they're waiting for IT companies to make massive rollouts of trust technologies; and they're waiting for governments and societies to agree on accountability measures. Meanwhile, companies like Heartland and P&G are on their own.

But there are things users can and should do, Scherlis contends. "The key phrase is 'configuration management,' " he says.

"People underestimate the impor-

Continued on page 28

END-TO-END TRUST

Last year, Microsoft published a paper outlining a concept that it dubbed "end-to-end trust," whereby strong authentication could protect every boundary and layer – hardware, software, people and data – in computing. It's an ambitious idea, but many of the pieces already exist, says Steve Lipner, Microsoft's senior director of security engineering strategy.

For example, Lipner has a Trusted Platform Module installed on his laptop PC. The TPM, from Trusted Computing Group, a nonprofit industry standards group, is a tamperproof microcontroller that can store a user's keys, passwords and digital certificates.

"It can validate that the software loaded at boot time is the one I think it is," Lipner says, "and it releases a cryptographic key that will decrypt my hard drive before I start to use my machine."

The device uses BitLocker software from Microsoft's Windows Vista and Windows 2008.

"That's a start," Lipner says. "But when we talk about the full end-to-end trust vision, we are also talking about being able to authenticate a lot more of the software on the machine, maybe all of it. We are researching the deeper integration of the TPM mechanisms."

Wider deployments of these mechanisms could show up in the TPM device itself, the operating system or third-party software, or in the form of new Internet standards, Lipner says.

However, in the short term, users must do the best they can with existing technology, says Alan Paller, research director at the SANS Institute, an information security education firm. He says cyberthreats that exploit software are of three types: those that exploit vulnerabilities left by faulty coding, those that exploit logic errors in faulty designs, and social-engineering exploits that trick users into doing things they shouldn't do, such as revealing a password.

"The most powerful of the new attack techniques are in social engineering, where they are doing much deeper analysis of the people they are going to attack," Paller says. But part of that is pure technology, he says, "because once you let the guy in, he still has to break some things."

That means defensive technology is needed inside the system so if, for example, a user clicks on some malware, the attacker can't then insert a keystroke-logger or other malicious software.

– GARY ANTHES

TEACH YOUR CHILDREN WELL

In January, The Mitre Corp. and the SANS Institute published a list of coding mistakes that make software vulnerable to attack; it was called the "Top 25 Most Dangerous Programming Errors."

Alan Paller, research director at SANS, says universities do a poor job of teaching students how to avoid those mistakes. "There is nothing nearly as important for improved security of software than getting [universities] to take responsibility for the lack of secure coding skills of their graduates," he says.

But Fred Schneider, a computer science professor at Cornell University, disagrees. He teaches a computer security class that covers sound coding practices, but he says a university's role is "teaching ideas and principles and how to think about things."

> **"There is nothing nearly as important for improved security of software than getting [universities] to take responsibility for the lack of secure coding skills of their graduates.**
> ALAN PALLER, RESEARCH DIRECTOR, SANS INSTITUTE

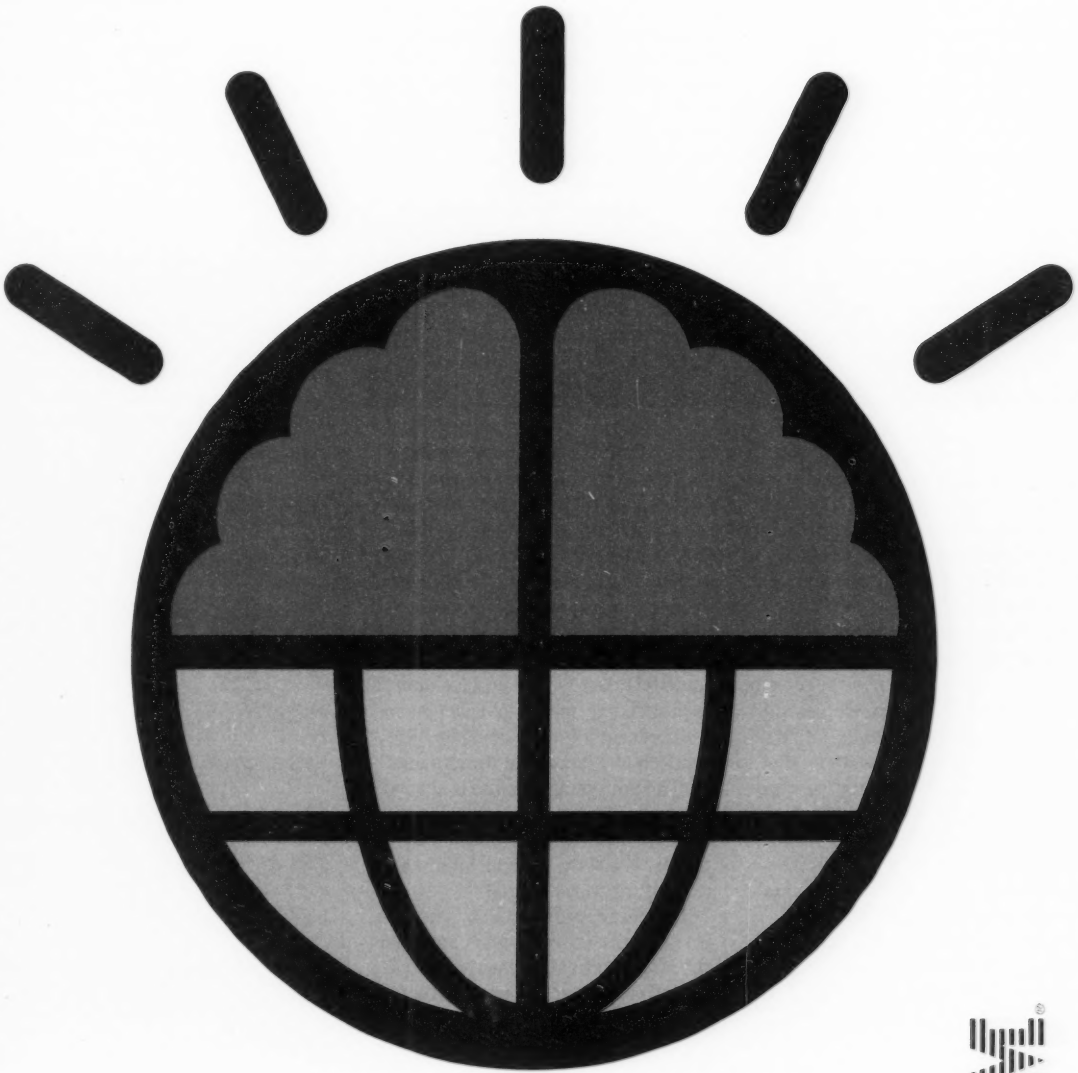
Schneider says software vendors often send new hires to training classes to learn secure coding practices, and that's as it should be.

But Schneider and Paller agree on at least one thing: While quite a lot is known now about secure coding practices, there is little agreement on what makes for a secure system design. "Nobody understands what it is about an architecture that contributes to a system being secure," says Schneider. "It's hard to recognize a bad design if you don't know how to tell a good design when you see it."

Says Paller, "There are ways to write secure code, but on secure design, there are only opinions. The guys with the opinions all think they are the only ones who know how to do it, and they don't speak to each other."

– GARY ANTHES

Managers spend up to two hours
every day searching for information,
over half of which has no value to them.
A smarter planet needs smarter IT.
Let's build a smarter planet.
ibm.com/intelligent



THINK

IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.
A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

NEEDED: INFORMATION, UNDERSTANDING AND MONEY

Experts in computer security generally agree that certain fundamental steps by industry, governments and society could go a long way toward solving the cybercrime crisis.

Those steps include adopting new views on the trade-offs between anonymity and accountability, building trustworthy systems from top to bottom based on strong authentication, employing only the latest and best techniques and tools in software development, and documenting and certifying designs and code.

The problem is that these things require strong commitments by multiple parties, and they require expenditures of considerable sums of money over a number of years.

Cornell University's Fred Schneider says federal funding of computer security research has been inadequate. He advises the federal government on such matters but, he says, "as a scientist, it's not my job to make trade-offs given fixed resources – to decide, for example, whether we should send troops into Afghanistan, help the poor or make investments that promote cybersecurity."

Schneider says that most people don't have an accurate understanding of the costs and risks of our growing dependence on untrustworthy systems because they don't know the extent to which systems control things, nor do they understand the magnitude of the threat. "Society doesn't really have sufficient information to make good decisions about the trade-offs," he says.

– GARY ANTHES

Continued from page 26

tance of this because it sounds dreary and dull — like taking inventory. But few organizations or users even know what's running on their computers," he says. "Stuff just turns up, and you don't even know what its heritage is."

Scherlis says that a typical desktop can have 5,000 or more executable files, many of them of uncertain origin. In addition, there are hidden files and dynamic modifications to files. "That's pretty scary," he concludes.

"Attend to the provenance" of your software, Scherlis says, and "be absolutely rigorous about configuration management and configuration integrity, both during development and ceaselessly during operations."

In the meantime, he says, an emerging idea is for builders of software to produce evidence that their code meets certain criteria. Developers can help buyers and users evaluate software by providing test cases, models, linked documentation such as Javadoc, development and configuration logs, bug and problem logs, and analysis results, Scherlis says.

But even the best protective measures will never completely do the job, says Robert Lucky, a research vice president at Telcordia Technologies Inc. in Piscataway, N.J. Lucky chaired a U.S. Department of Defense task force in 2006 that looked into the threat from malicious code secretly inserted in U.S. software developed abroad. His report detailed a number of steps that could be taken to help protect against such sabotage, but he told *Computerworld* recently that he considers the problem of cybercrime "intractable."

"The bottom line for me is always risk assessment," Lucky says. "You can't spend an infinite amount of money. You have to make intelligent trade-offs and accept risk."

The best approach, Lucky suggests, is to identify those system components that are critical and sensitive, and "spend the big bucks" only on those. But he acknowledges that it's not easy to list all the critical components in a large, complex system.

No matter what users and vendors do, Cornell's Schneider warns against complacency. Schneider, who chairs Microsoft's external advisory board on security, says, "It's clear [Microsoft's] software is much more secure than it was five years ago — no question." But whether software is more secure is not the right question to ask, he says, "because the threat has changed, too."

Software has gotten better, and that's nice, he says, but it's "getting more complex, and the rate of successful attack seems to be increasing."

The challenge today is to approach the problem more holistically. And we'd better hurry, Schneider says, because the bad guys are going to get a lot more knowledgeable.

"There are lots more sophisticated methods of attack that they don't yet use," he says. "Our software could get better, and they would still have many tricks." ■

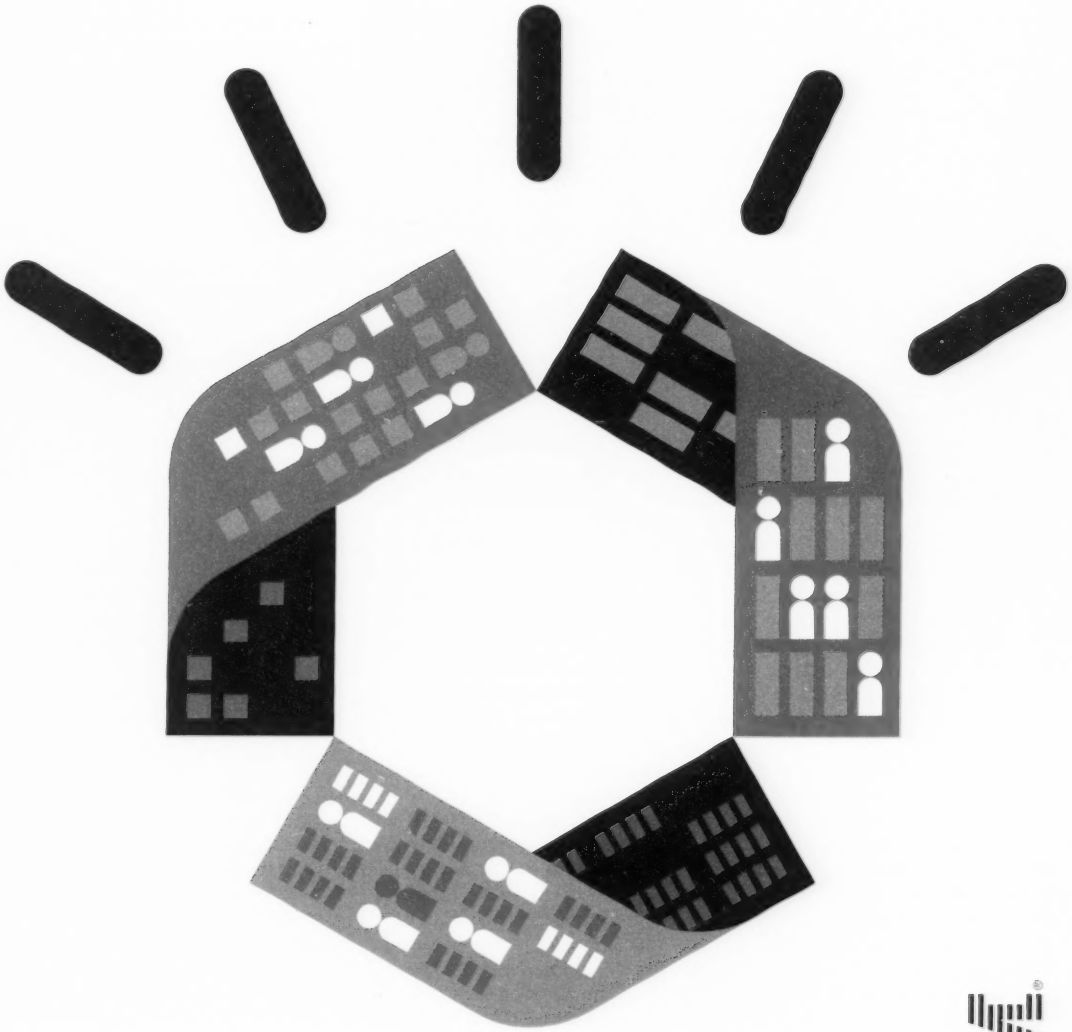
SKIRMISHES

According to the Computer Security Institute's 2008 Computer Crime and Security Survey, the following percentages of respondents reported experiencing these types of incidents in the previous year.

Virus infection	50%
Laptop theft	42%
Unauthorized access	29%
Targeted malware attack	27%
Denial-of-service attack	21%
Bots	20%
Theft/loss of customer data	17%
Abuse of a wireless network	14%
System penetration	13%
Financial fraud	12%
Theft/loss of proprietary information	9%
Password sniffing	9%
Sabotage	2%

BASE: 522 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities. Multiple responses allowed.

By 2011 there will be 2 billion people
and 1 trillion connected objects on the Web.
A smarter planet needs smarter IT.
Let's build a smarter planet.
ibm.com/connected



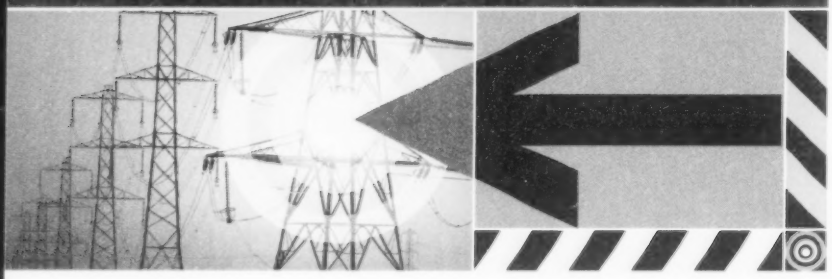
THINK

IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.
A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

SPECIAL REPORT

The New GROUND ZERO In Internet Warfare

The power grid is an obvious target for terrorists, but experts disagree about how to secure it. By Julia King



WHEN it comes to critical national infrastructure, the highly distributed and ultra-interconnected U.S. power grid is, hands down, the most vulnerable to cyberattack. On this one point, many cybersecurity experts seem to agree.

Yet just how likely a terrorist target is the grid? And what's the best way to secure and protect the massive inventory of generators, power plants and transmission lines, plus the cat's cradle of computer networks that make up the electric power system?

Talk to 10 experts, and you'll likely get 10 different answers.

"The problem is that we have a hard time assessing risk," says Jim Lewis, a senior fellow specializing in cybersecurity at the Center for Strategic and International Studies. "We seem to settle on either indifference or a Bruce Willis movie."

Up until about a decade ago, things were a lot simpler. The industrial controls that managed the generation and flow of power were protected from intrusion by their closed-loop architecture. Those control systems operated in isolation from everything else.

But those systems have been increasingly linked to countless corporate networks for everything from real-time monitoring of electricity generation and transmission to remote meter-reading and automated grid operations. "We had an explosion in business network technology, and as that occurred, individuals in accounting, for example, wanted real-time information at their desktop computers so they could do projection planning," says Michael Assante, chief information security officer at North American Electric Reliability Corp. (NERC), an industry organization of electrical grid operators.

Today's so-called smart grid relies heavily on public communications networks, including cellular networks and WiMax, to digitally monitor and control the grid for more efficient operation, he explains.

But more connections mean more points of vulnerability, and that's what worries Sami Saydjari, president of Cyber Defense Agency LLC, a privately held security consulting firm in Wisconsin Rapids, Wis.

"The power grid is controlled by systems that are antiquated and highly vulnerable because they have very little security. They've been historically protected by disconnection," he says. But the rush to improve convenience and efficiency by linking administrative and billing systems via the Internet has created gateways to the power grid controls, Saydjari notes.

"The concern that many of us have is that an adversary can jump that gap directly or indirectly and exploit vulnerabilities," he says.

In particular, they could use the control systems to disable physical things, like generators, or overload transformers and destroy them, Saydjari says. If that were to happen, it could take six months to replace transformers or generators, "and we have no [replacement] manufacturing capabilities in the U.S.," he says. "Germany, China and Japan are our sources."

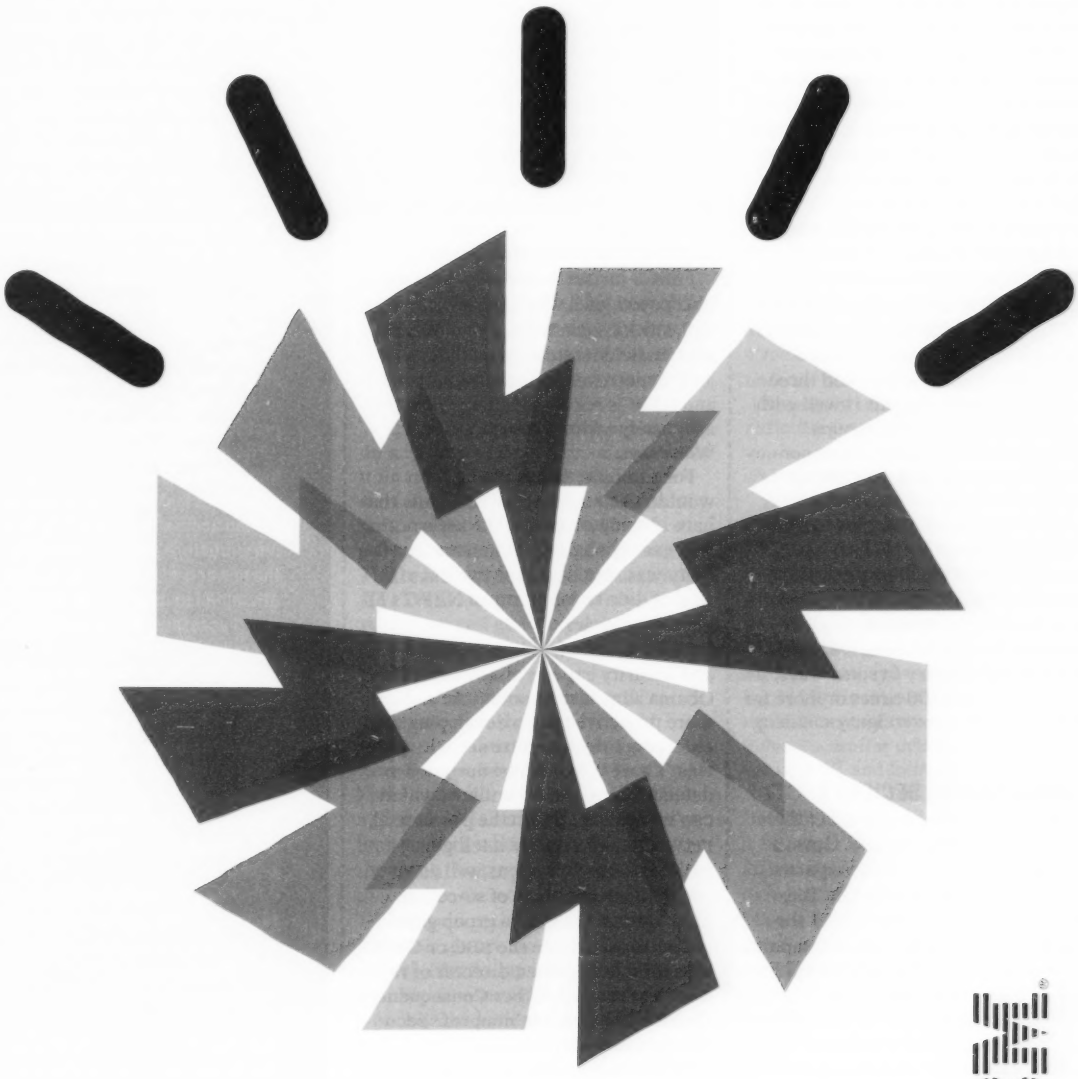
CASE IN POINT

An incident illustrating the types of vulnerabilities attackers could exploit took place last March in Baxley, Ga. The Hatch Nuclear Power Plant was forced to shut down for two days following a glitch that occurred after a software update was installed on a computer on the facility's business network. When the computer rebooted, it reportedly reset the data on the control system but also caused the control system to misinterpret dropped data as a drop in the water reservoirs that cool the plant's radioactive nuclear fuel rods. Mistakenly sensing a drop in the water reservoirs, the plant's safety systems triggered a shutdown.

Industry officials readily acknowledge that it's indeed possible to break into the control systems via the Internet and cause damage. But surprisingly, they also contend that it's highly improbable that a cybercriminal or terrorist would target the electric grid.

Continued on page 32

It's estimated that the world's datacenters will produce more carbon in a year than the total electricity usage of 36 million homes.
A greener planet needs smarter IT.
Let's build a smarter planet.
ibm.com/efficient



THINK

IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.
A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Continued from page 30

"The average attacker is trying to gain financially from illicit activity," says Assante. That explains why attacks on financial institutions and e-commerce operations are far more frequent than attacks targeting electric utilities. Power systems "aren't a good place for a cybercriminal to monetize their efforts," Assante says.

Terrorists generally "want to do things cheaply and quickly," says an industry official who requested anonymity. To figure out how individual electric companies protect their portions of the grid and how they're connected into regional operations would require "a lot of time, money and hard science," the official says. "From a terrorism standpoint, it's far more likely that they'd drive a truck into a generation station or shoot guns at a nuclear facility."

But Saydjari maintains that a terrorist attack on the power grid would do catastrophic damage. He estimates that such an attack would require about a half-billion dollars and three years to execute, "but this is well within the means of terrorist groups."

"Some studies indicate that a concerted strategic attack could bring down 70% of the power grid for six months or more," Saydjari says. "This would be devastating to the country. Just think about what happened during Hurricane Katrina. When you take away power from a region, civilization degrades. During Katrina, we had a Third World country in some ways. If you multiply that 100 times or more for six months, it's a sovereignty-challenging event."

STANDARDIZING SECURITY

So, what's being done to protect the grid? For one thing, the U.S. Government Accountability Office reported on security weaknesses at the Tennessee Valley Authority (TVA), the nation's largest public power company. Then in January 2008, the Federal Energy Regulatory Commission (FERC) approved eight mandatory reliability standards that NERC developed to protect bulk power systems against disruptions from cyberattacks.

Electric utilities must comply with NERC's so-called CIPS — critical infrastructure protection standards — several of which focus on cybersecurity.

"Standards lay the foundation [for cybersecurity]," says Assante. "What makes the power system unique is that it is so interconnected. From a security context, there's the weakest-link argument. That's why we have to have everyone doing the same thing."

Prior to 2005, electric utilities were self-regulating, checking up on one another's compliance with NERC-sanctioned security recommendations. Now, however, violations of the mandatory reliability standards approved by FERC carry fines of up to $1 million per incident per day. "There are some very serious teeth," says Assante.

Still, the current regulatory environment has its share of critics, including Joe Weiss, a control systems engineer and managing partner at Applied Control Systems in Cupertino, Calif.

FERC's jurisdiction covers only the bulk power grid, which includes federal entities such as the TVA, Weiss says. Individual states and NERC share jurisdiction over power distribution, and NERC's regulations simply don't adequately address control systems, Weiss says.

For example, "the NERC CIPS wouldn't have prevented incidents that have already occurred," he says, noting that even though the Hatch nuclear facility was shut down for two days last year, it didn't violate any of NERC's IT security policies.

Looking ahead, industry officials and security experts alike expect the Obama administration to take a much more proactive role in developing and enforcing infrastructure security policies. Those rules will be designed to defend against cyberconflicts, which can involve attacks on the power grid, network operations or intelligence-gathering capabilities, as well as terrorist attacks and acts of so-called hacktivism, in which "a group gets together to take down the BBC or CNN," says John Bumgarner, director of research at the U.S. Cyber Consequences Unit, an independent nonprofit security research organization.

"The Obama administration is going to be doing a lot with cyber-type activities," says Bumgarner. "Obama is our e-president. He understands technology." ■

NOT JUST HYPOTHETICAL

Last month, when *The Wall Street Journal* reported that Chinese and Russian adversaries are regularly hacking the U.S. power grid and seeding it with electronic time bombs, John Bumgarner was not the least bit surprised.

"It's a known fact that our critical infrastructures are being probed and penetrated by adversaries on a regular basis," he says. "Every day, a critical infrastructure in the U.S. is probed by somebody."

What is new, he says, is the growing number of officials in government, the utilities industry and elsewhere who are willing to acknowledge the vulnerabilities. "It's not just the CIA anymore," says Bumgarner, director of research at the U.S. Cyber Consequences Unit, an independent nonprofit security research organization.

The *Journal* quoted unnamed intelligence officials as saying that foreign operatives last year had repeatedly gained access to several U.S. critical infrastructure systems, including the power grid. "The Chinese have attempted to map our infrastructure," according to the senior official quoted.

Commenting on the report to ABC Television, former presidential cybersecurity expert Richard Clarke said it has been known for some time that foreign governments have been setting up what he calls "offensive cyberwar units." He also says the U.S. power grid is "pretty easy to penetrate."

One way to reduce or prevent attacks is to "disconnect the power grid control system from the Internet," Clarke suggests.

However, Bumgarner notes that such a remedy is unlikely to be implemented because identifying and disconnecting all the Internet connection points supporting the power grid would be almost impossible, especially during a period of national crisis.

– JULIA KING

Russia's CYBERBLOCKADE Of Georgia Worked

Lesson learned: DDoS attacks, as well as the response to them, can cripple a country.
By Patrick Thibodeau

THE RUSSIAN-GEORGIAN war of last August began in cyberspace, with Russia launching sporadic denial-of-service attacks targeted primarily at Georgian news and government Web sites weeks before the shooting started. And at first, says Eka Tkeshelashvili, secretary of Georgia's National Security Council, the Georgian government wasn't certain what to make of the situation.

Officials believed that Russia was attempting to apply psychological pressure on their country and cause some disruption, "but not to the extent that the whole banking system would have been shut off, crippling the economy," says Tkeshelashvili.

But that's exactly what happened. As armed hostilities began, the distributed denial-of-service (DDoS) attacks increased in severity, making news and government Web sites impossible to reach. Banks shut down servers to protect themselves from the theft of data, but a flood of false information and erroneous IP packets presumably originating in Russia triggered an automated response from international banks to sever connections to the country.

By itself, the DDoS attack was affecting Georgia's ability to reach the world, but the problem was compounded by the reaction to the attack from financial institutions. Combined, these actions had one result: Georgia became isolated.

After taking Georgia offline, Russia, in a sense, had the Internet to itself. In the initial days of the fighting, the Russian news media could present its version of the war while the Georgians dealt with what amounted to a cyberblockade.

"There is no way that Georgia could do anything at all to stop or reverse the military defeat that was staring it in the face," says Patrick Worms, a communications adviser to the Georgian government at the time of the war. The only thing it could do was generate global condemnation of this Russian move and global sympathy for its plight, he says. But to do that, it needed Internet access.

Russia's attack was intended "to make sure that the outside world couldn't see into Georgia and make sure Georgia couldn't get in touch with the outside world," says Tom Merilo, a retired Bell Canada information systems auditor who was in Georgia after the war to help with technical efforts to improve the networks.

The main paths for network access into Georgia are through Russia and Turkey, Merilo says. Routers in Russia or otherwise outside Georgian control were hijacked and traffic was rerouted, making even connecting to Internet-based e-mail accounts, such as Gmail, difficult to impossible.

Volunteers, many from outside Georgia, helped to set up mirror sites by redirecting domains to new hosting providers in other countries. For a time, the Web site of Georgia's foreign ministry was hosted on Google's Blogspot service. It was a "whatever works" approach, and within a few days of the initial attack, Georgia began regaining some ability to communicate with the outside world via the Internet.

HARD LESSONS

Worms believes the lessons from the attack are "extraordinarily significant." A DDoS attack "is so easy to set up, it's so easy to activate, and it is so potentially effective that any country is at potential risk of serious disruption from these tools," he says.

Stephen Spoonamore, a security expert and partner at Global Strategic Partners LLC in Washington, argues that the "echo" effects of such an attack, which in the case of Georgia included the shutdown of the financial settlement system, can be just as destructive, if not more so, than the attack itself.

He says the use of cyberattacks by nation-states will only grow. "I think you are going to see it on a regular basis now, because it works," he says.

Meanwhile, in Georgia, "we have to be prepared for everything," says Tkeshelashvili. The country is working to "integrate all the measures" available so it can better protect itself from future cyberattacks, she says.

Georgia is a small country without a sophisticated cyberdefense capability, but NATO is taking the incident seriously. Russia is believed to have been behind a similar cyberattack in Estonia in 2007, and following that event NATO created the Cooperative Cyber Defence Centre of Excellence, which is based in Tallinn, Estonia. "The need for a cyberdefense center to be opened today is compelling," said Gen. James Mattis, NATO's Supreme Allied Commander Transformation, at the opening of the center last year.

Could something similar happen in the U.S.? One IT manager, a Georgian native who works here and didn't want his name used, says it's entirely possible that foreign governments today have hundreds of servers in various commercial hosting sites in the U.S. prepared for just such a thing. ■

Internet INTERRUPTUS

'The Internet is down.' What does that really mean? By Russell Kay

YOU TYPE a URL into your browser or click on a link. Then you wait an instant or two while your page loads. But sometimes you keep waiting. Or you get "Error 404: Page Not Found." Possibly, your browser times out while waiting for the server to respond. We tend to summarize all these events with a simple phrase like "The Internet is down."

In almost all cases, that global interconnection of networks that gives us the World Wide Web, e-mail and countless other online services is still operating. The Internet is still there; we just can't get to it. But why?

The root cause could be almost anywhere. The culprit could be something inside your computer or attached peripheral equipment, or a service interruption from your own network or ISP. It could be a regional or wider-scale outage caused by faulty equipment, weather problems or accidental or malicious damage to cables, or a disruption caused by malicious software such as a virus or a Trojan horse. Or it could be something as simple as the need for routine maintenance.

POSSIBLE POINTS OF FAILURE

Inside your local system and close by: A hardware component or connection failure is a real possibility. If the hardware is OK, how about your software? Windows is notorious for slowing down over time. How long has it been since Windows was installed or since its registry was checked for inconsistencies and cleaned out? Have you installed the latest service packs and patches to your operating system and browser? Is your antivirus, antispyware and firewall software up to date and working?

Regional upsets: The problem could lie with your office network or ISP. A quick phone call to the help desk or your ISP will let you know.

WHAT TO DO?

When you lose Internet service, follow these steps before you call for help:

- **Wait a few minutes; many Internet outages resolve themselves in short order.**
- **If you get a timeout message, try again right away.**
- **Check all I/O cables, including those attached to your PC, router, network, and cable or DSL modem.**
- **If you're on a wireless connection, try plugging in with a cable.**
- **Unless there's a good reason why you cannot or should not do so, try restarting your computer and, if applicable, your router and/or modem. Restart, don't reset: Just unplug them, wait 30 seconds, then plug them back in and let them reboot. Nine times out of 10, this will fix the problem.**

– RUSSELL KAY

Their problems could involve hardware or software. Service might be down because of severe weather, a power outage, or physical damage to a data center caused by anything from an accident to an act of God to an act of terrorism. In 2007, an electrical outage in San Francisco took down a data center hosting a number of popular sites, including Craigslist, for several hours.

Major service-provider outages: Simple things can have unexpected consequences, especially for major service providers. When Google tested new software during regular data center maintenance in February, millions of users lost access for more than two hours.

Similarly, in 2008 a two-hour global Hotmail outage occurred that also affected MSN Messenger and other Microsoft Live services. In July 2001, MSN Messenger was down for about a week for some users after a disk controller in a database server failed.

Amazon.com Inc.'s S3 cloud computing service, which provides on-demand storage, suffered an outage in February 2008 when a data center's authentication service was overloaded. Subsequent outages at Amazon led to speculation that the company was the target of a denial-of-service attack.

A software failure took down parts of eBay for almost a day in 1998. After similar problems in 1999, 2002 and 2003, the company created an outage policy for customers and reassured investors that it had resolved reliability issues.

International connections: Despite the wide use of satellites and wireless communications, global communications still depend heavily on fiber-optic cables that connect continents. In December, millions of Web users in the Middle East lost connectivity when a string of underwater cables in the Mediterranean Sea was damaged. As much as 70% of all Internet traffic and telephone communications between Europe and Africa was affected, and Internet traffic had to be rerouted through Asia and the U.S. Similar cable damage had occurred less than a year before, when ships' anchors had torn through a different section of those same cables. ■

Kay *is a Computerworld contributing writer in Worcester, Mass. You can contact him at russkay@charter.net.*

In the Trenches, as The Threats Evolve

We've gone from **free-floating malware** to **targeted attacks** to **organized international crime.** What will be next?

RECENT security incidents at my company have gotten me thinking about the state of information warfare (see special report, page 22). Electronic break-ins are progressing in a direction that makes me fear that the nature of the threats is changing.

Only a couple of years ago, incidents were largely virus- and worm-related. Although an outbreak of network-borne malware could bring a company's IT infrastructure to its knees, sometimes for days, those were never targeted attacks.

Most were simply the random exploitation of flaws in popular operating systems, browsers or software, perpetrated by what we imagined were (and what usually turned out to be) bored teenagers with too much time on their hands and access to rootkits, exploit code and virus-creation tool kits. Random malware just floated on the electronic breeze, sort of like — well, like a virus.

Then, the landscape changed. I started seeing manually executed attacks. At first, they were either practical jokes perpetrated by someone who knew the victim, or random poking around by somebody in proximity to the target. That was the first major change in the attacker-target relationship — the attacker had some connection to or familiarity with the target. The motivation was the pride to be gained by proving one's skills.

In one investigation, I determined that the target — whose workstation had suddenly started giving him a message that he was "0wned" — was the victim of an intradepartmental contest of pride between two systems administrators. Sadly, this now seems harmless.

I first ran up against an international attack three years ago. Some of our company's laptops were storing large data files that upon investigation turned out to be DVD copies of movies that were still in the theaters. We eventually discovered how this had happened. On those laptops, our IT department had rolled out a sales force automation package that relied on database software whose administrative password was left blank and whose administrative command set allowed full access to the laptop.

■ Random malware just floated on the electronic breeze, sort of like – well, like a virus.

It was a fairly simple matter for the movie thieves to use this oversight to do whatever they wanted with the machines once they found them. But what was notable was the location of the attackers: Germany.

Because of the international nature of this incident, our legal department decided not to pursue prosecution, and other than blocking access, we did nothing more. But look at the evolution of motivation and scope: Our attackers were from outside the U.S., no longer close to their victims in any sense, and they reached out across thousands of miles to steal computing resources.

Trouble Ticket

AT ISSUE: The threat landscape is constantly changing.

ACTION PLAN: There's no way to know what will be thrown at you; just be prepared for anything.

Since then, of course, things have escalated into international phishing, pharming and those ubiquitous Nigerian bank scams. In my mind, they represent a snowballing of the international scope and reach of today's threats.

I don't really have to tell you anything about those sorts of attacks, but I will tell you about an interesting type of attack I've been dealing with over the past few months. This one is an extortion scheme from China.

A message arrives with an official-looking and professional-sounding letter, stamped with the Great Seal of Somebody Significant, demanding that our company pay a settlement fee in order to resolve a dispute involving our corporate domain names. This type of incident is financially motivated, international in scope and fairly sophisticated in appearance.

Now that our threat landscape has evolved from simple, random network malware to targeted attacks and then to increasingly organized international crime, I can't help but wonder what's next. ■

This week's journal is written by a real security manager, **"J.F. Rice,"** *whose name and employer have been disguised for obvious reasons. Contact him at jf.rice@engineer.com.*

COMPUTERWORLD.COM

JOIN IN

To join in the discussions about security, go to **computerworld.com/blogs/security**

■ OPINION

Paul Glen

Five Clues a Project Is Headed for Trouble

IN THESE DIFFICULT TIMES, lots of projects are getting canceled, postponed or mothballed. Although these are perfectly normal occurrences in IT, they seem more frequent, swift and stinging now.

When a project is killed, we like to think that its fate is entirely due to external forces — the swirling, uncontrollable winds of the economic hurricane happening outside. It's not that we're doing anything wrong, we reason; it's just a response to the crisis.

But in those fleeting moments of honesty, those quiet times awake in bed at 2 o'clock in the morning, we know better. Many of those projects weren't selected for cancellation just because of sudden shifts in priorities. Some of them were canceled because there were problems. They were judged unlikely to ever be completed. Or they were expected to exceed time or budget constraints, or to fail to offer sufficient business value even if they did deliver a product.

So in these austere times, it's more important than ever to recognize project problems early so that you can correct them or at least cancel the project before wasting too many resources.

Yes, we all know that something's wrong with the project when we blow a budget or miss a major deadline, but how can we know before it's too late to do something about it? Here are five early warning signs that your project is in trouble:

1. Management direction is inconsistent or missing. If project leadership has gone AWOL, chances are that things are starting to go in a bad direction. Or, even worse, if the directives you get from management (or feel compelled to give if you are management) change frequently, there's a problem. If a project either lacks direction or can't maintain a reasonably consistent course, it's unlikely to get to any desirable destination.

2. Project management and business management seem disconnected. Even if a project does get consistent direction, if that direction seems to be at odds with business management's desires, there's a problem brewing. In political battles between IT and business management, business management usually wins, even if it takes a while. I don't hear too many stories about the great political triumphs of IT managers over their users or clients.

■ In political battles between IT and business management, business management usually wins.

3. The team lacks a commitment to clearly articulated and commonly understood goals. Every project has a goal or two. They may be clearly stated or only vaguely discussed, but it's rare for any business to shell out lots of money for something that genuinely has no purpose. That said, it's common to presume that the purpose of a project is so obvious as to not be worth articulating. That's unfortunate. It typically leads to misunderstandings and inconsistent presumptions about priorities. Eventually, poor and inconsistent tactical decisions undermine project progress.

4. Team members don't listen to one another. Even when teams get along personally, team members don't always listen well to one another. This tends to lead to chaos as people fail to coordinate activities and make the compromises necessary to enable projects to move ahead.

5. The team is in a state of discord. Teams sometimes break into competing camps. These can form around honest-to-goodness differences over project direction. They can also form over petty loyalties and personality clashes. Sometimes teams just descend into chaos, with multiple factions or an every-person-for-himself ethos. The state of discord is destructive to progress. It needs to be rooted out. Sometimes, as a manager, you can engineer a reconciliation. Other times, you need to pick winners and losers.

If you notice any of these things happening on your projects, the time to act is now. Don't wait until it becomes obvious that the project is a disaster in the making. By intervening at the first sign of trouble, you may be able to save both projects and careers from the swift executions going on today. ■

Paul Glen *is the founder of the GeekLeaders.com Web community and author of the award-winning book* Leading Geeks: How to Manage and Lead People Who Deliver Technology *(Jossey-Bass, 2003). Contact him at info@paulglen.com.*

Career Watch

Don't Twitter Your Job Prospects Away

Do you doubt that things move fast in our highly connected world? In mid-March, someone with the username of "theconnor" posted a public tweet on Twitter: "Cisco just offered me a job! Now I have to weigh the utility of a fatty paycheck against the daily commute to San Jose and hating the work." Tim Levad at Cisco saw the tweet and replied, "Who is the hiring manager. I'm sure they would love to know that you will hate the work. We here at Cisco are versed in the web." And that same day, someone else established the Web site CiscoFatty.com and shared the story. No one seems to know whether theconnor (or Cisco Fatty, if you prefer) took the job or not, but he or she did learn a lesson and instituted some privacy settings on Twitter. Of course, there's a lesson for us all – to watch what we say and to whom.

Are Layoffs Too Expensive?

Maybe some IT jobs will be saved if enough executives read a March 8 research note from AMR Research Inc.'s Phil Fersht and then are able to convince the top brass of the sense of Fersht's argument. Which is this: The cost of laying off an IT employee may exceed the benefit to be derived. He says that should the economy recover in 2010, a company might derive only $50,000 to $100,000 in savings from each IT layoff, after all costs have been incurred. Then Fersht asks how those savings stack up against the cost of replacing the laid-off employee once conditions improve. "How can you put a price on replacing the inherent business knowledge of that staff member when you rehire a replacement?" he writes. "It may take another year or two to get the replacement up to speed, and will not only end up costing you more, but may also impede your executives from accessing critical data in a timely fashion. The overall cost of replacing that staff member could easily be three times the costs saved by laying her off. And these easily-identified direct costs are only the beginning; the costs incurred to your culture and morale can prove even more damaging."

PHOTOGRAPH: MARTIN HOOPER

■ Q&A

Steve Gaudino

The COO of **Training Camp** talks about certification programs for unemployed IT workers.

You market your courses as being "boot camp style." What does that mean? We try to take an existing [certification] program and accelerate it. All of our classes are residential, so you would come and stay with us for a period of five to 14 days, depending on the program. We run classes from about 8 in the morning to about 9 at night. We try to stuff as much information as we can into those hours and make sure that not a minute goes wasted.

Companies often cut back on training in tough economic times. How has that affected your business? Business spending has cut back a little bit. But typically what we find is when business spending cuts back, we usually get more individuals, because people have either been laid off or they're concerned about being laid off. So instead of the company paying for it, the individuals will be the ones paying for it. Our revenues year-over-year have pretty much been flat.

Up until about a year ago, we were probably about 80% employer-funded and 20% employee-funded. Recently, it has been more like 60% corporate and 40% individual. We have seen a fairly nice uptick lately in government spending – particularly, the military branches have been giving us a bunch of business. They're the one sector that seems to always be immune.

Are you finding that people are switching from less recessionproof careers into IT? Sure. There's a ton of examples, but one that comes to mind is a real estate agent who recently came through. With the housing market the way it is, she wanted to get into a new career, and the path she chose was technology. She had some interest in computers already, and she felt that with this cert, she could make herself marketable for a potential help desk role.

You recently announced a plan to offer free hotel accommodations for unemployed workers. What's the fine print? No fine print. As long as we can get some adequate documentation or otherwise believe the student is unemployed, we're going to help him pay for his training by covering the cost of his hotel and/or exams for him, depending on the program and what that student needs.

And to those who suggest your plan is more marketing than altruism? Well, we're obviously taking money out of our pocket to pay for the hotels or exams. The other thing we're doing is if someone comes and takes a class and ends up getting laid off, we're extending another free class for them that they can take down the road. So while we may enjoy some positive press out of this and may get some additional business, at the end of the day, we're putting our finances on the line. We're trying to help out.

– DON TENNANT

PAGE COMPILED BY JAMIE ECKLE

Computer

RCG Information Technology, Inc. an industry leader, we are able to provide our people with the kind of work environment others can't match. We are looking for the following IT professionals with >1 year experience, for our New York, New Jersey, Illinois, and Pennsylvania offices.

Programmer/Analyst; Systems Analyst; Database Adm.; Database Analyst; Lan/Wan Adm.; Software Engineer; Web Developer; Data Warehousing Architect; Business Analyst; Solutions Sales Execs; QA/Tester; QA Analyst; Technical Recruiter

Needed skill sets:
Client/Server, ERP-SAP, Oracle, PeopleSoft, Internet, E-Commerce, Mid-Range, AS/400, CRM-Siebel, Data Modeling

Please e-mail your resume to: rirjobpost@rcgit.com referencing Job Code: PrintAdCW. We are an Equal Opportunity Employer. M/F/D/V

With 35 branch offices located across the US, COMSYS is actively recruiting for the following positions.
Business Analyst– metro Jersey City, NJ– Code # JC100
Database Administer– metro Houston, TX – Code # HO150
Business Systems Analyst– metro Oklahoma City, OK– Code # OC100
Programmer Analyst – metro Phoenix, AZ– Code # PH120
Systems Administrator – metro Charlotte, NC– Code # CH140
Roving employment to varying jobsites throughout the US. Please refer to appropriate job code when submitting resume to: COMSYS, Attn. Nancy Theriault, 15455 N. Dallas Pkwy., Ste 300, Addison, TX 75001. EOE./MF/DV

Software Project Manager w/ Masters in Comp Sci or Engg & 1 yr exp. Plan, organize, direct & coord. IBM MQ, WebSphere Application Server. Engr & dsgn s/ware for automated provisioning of IBM MQ, IHS, WebSphere Application & Portal Server builds. Perform third level problem resolution; performance tuning & analysis using Tivoli & Wily Introscope. Engr end-to-end secure integration solutions for WebSphere w/iPlanet, LDAP, DB2, & Oracle. Dvlp, maintain & track comprehensive project plans. Supv 2 Consultants. 1 yr exp as Lead Engr acceptable. Mail res to: Open Systems Technologies, 462 7th Ave, 15th Fl, NY, NY 10018. Job Loc.: NYC or in any unanticipated locs in the USA

IT MANAGER w/Masters in Comp. Sci or Engg & 6 mos exp. Implmt Business Intelligence projects, use SDLC techniques & gather reqmts to production implmtn. Dvlp, test & administer corp. BI applic. Dsgn BI applic objects using relational d/bases & data model/data warehouse concepts. Dvlp & deploy an enterprise wide BI user interface using XML, XSL, HTML & ASP web customizations. Use SQL to troubleshoot BI issues. 6 mos exp as IT Analyst acceptable. Supv 2 Consultants. Mail res to: iNINE Technologies LLC, 3 Independence Way, Ste #117, Princeton, NJ 08540. Job Loc: Princeton, NJ or in any unanticipated locs in USA.

Senior Developer: Strong programming and system analysis skills. Proficient in ASP, .NET, SAMLite and SQL 2000 in Windows. Exp. with .Net remoting, XML/XSL, LINQ, ASP and development of ASP.Net websites using VB.Net. Fax resume (954-783-6230) Gary Youngman, Dealer Data, 950 N. Federal Hwy., Suite 207 Pompano Beach, FL 33062

Nabors Corporate Services seeks Oracle Database Administrators to work in Houston, Texas. Plan, coordinate, maintain and support of Oracle E-Business Suite, and Oracle Databases for UNIX and Windows. Candidate must have a bachelor's degree in engineering or computer science plus 5 years progressive experience as an Oracle Data Base Administrator. Submit resume to Patricia Holloway at Patricia.Holloway@nabors.com. **Must put job code NCS09DBA on resume.**

Software Engineer w/Bach or foreign equiv in Comp Sci or Engg & 6 mos exp. Dsgn, dvlp, test, implmt & analyze bus. s/ware infrastructure solutions using J2EE, LDAP, Oracle, Unix, C, C++, Perl, Shell Scripting, XML, Servlets & SAP R/3. Perform integration & deployment using Java Enterprise products (Directory Server, Identity Mgr, Access Mgr, Application Server). 6 mos exp as Prgmr Analyst acceptable. Mail res to: MGL Americas, Inc, 220 Old New Brunswick Rd, Ste #101, Piscataway, NJ 08854. Job loc: Piscataway, NJ or in any unanticipated locs in the USA

COMPUTERWORLD 100 BEST PLACES TO WORK IN IT 2009

Take this opportunity to show why your company is an employer of choice to the IT community!

Over 1,000,000 qualified IT professionals will be looking to this must-read issue for future career opportunities. Don't miss out on Computerworld's biggest and most anticipated career issue of the year!

Issue Date: June 15th
Space Deadline: June 1st

For details contact:
Dawn Cora at 508-820-8133
dawn_cora@idgcommunications.com

Labor Certification Ads

Are you an individual, agency or law office needing to place ads to fulfill legal requirements?

Let us help you put together an efficient, cost-effective program that will help you place your ads quickly and easily.

For more details, contact us at: 800.762.2977

IT|careers

Shark Tank

TRUE TALES OF IT LIFE AS TOLD TO SHARKY

Thanks, Boss – Really!

Management decides it's finally time to start pushing down Windows updates, and there are a lot of them since SP2. But one user is sure the endless requests to reboot must be from a virus. When this IT pilot fish tries to explain, user gets abusive and demands to speak to fish's manager. "I put the user on hold, went to my boss and gave her a rundown," fish says. "She picked up the line and this is what I heard: 'This is Alice. Yes ma'am, new update policy. No ma'am. No ma'am. [Louder, angry voice.] Ma'am, you have insulted and belittled my employee and myself. I am going to notify my vice president and your manager and recommend that disciplinary action be taken.' *Click*. The boss proceeded to use very colorful language, picked up the phone and lived up to her promise, starting with the VP. From then on out, we were told to hang up on people like this and report them."

A Little Too Much

Pilot fish passes along a message sent by his department's help desk to all employees at his location: "At 10:35 a.m., we had a power spike in the server room that caused most of the network equipment to go down. This affected network access to servers, Internet, e-mail, mainframe, voice-over-IP phones and most other network resources. This was an unexpected result of bringing up new network equipment for the network re-architect. This caused our UPS to go into error state and send a power spike. Some of the equipment could not handle this spike. We've temporarily migrated the power off of the failed devices and will schedule a time to migrate the power again after business hours. We will also be working with our UPS vendor to look at the UPS to verify why this happened and prevent it from happening again." Sighs fish, "Ninety-eight percent of these employees would have not one clue as to what was said in this message."

At Least He Asked

Malware from the Web is becoming a problem where this support pilot fish works. "We have about two tickets a week with users saying they have thousands of viruses and they need to download software," says fish. "Now, every machine has virus protection, and every one runs locked down in user-only mode to prevent the rogue installation of software. But we have decided we need to increase our user awareness after the following ticket: 'I just received an ominous warning that my computer was infected with several viruses. I tried running the program to remove these viruses (as it indicated for me to do), but I'm not sure it worked. I wanted to let you guys know in case there is something else I need to do.' "

■ *Do this: Send Sharky your true tale of IT life at sharky@computerworld.com. You'll snag a snazzy Shark shirt if I use it.*

COMPUTERWORLD.COM

NEED TO VENT YOUR SPLEEN?
Toss some chum into the roiling waters of Shark Bait. It's therapeutic!
sharkbait.computerworld.com

CHECK OUT Sharky's blog, browse the Sharkives and sign up for Shark Tank home delivery at **computerworld.com/sharky.**

■ COMPANIES IN THIS ISSUE

Page number refers to page on which story begins. Company names can also be searched at computerworld.com

AirStrip Technologies LP 17
Amazon.com Inc. 34
American National Standards Institute 11
AMR Research Inc. 37
Apple Inc. 6
AT&T Inc. 6, 17
Bell Canada 33
Broadcom Corp. 11
Cape Light Compact 20
CardioNet Inc. 16
Carnegie Mellon University 23
Center for Strategic and International Studies 30
Centers for Disease Control and Prevention 14
CIA 32
Cisco Systems Inc. 10, 17, 37
Computer Security Institute 28
Cooperative Cyber Defence Centre of Excellence 33
Cornell University 24, 26, 28
Corventis Inc. 16
Craigslist Inc. 34
Cyber Defense Agency LLC 30
Depository Trust & Clearing Corp. 23, 24
Dexterra Inc. 17
Directions on Microsoft 11
eBay Inc. 34
Emergin Inc. 17
European Commission 11
Federal Energy Regulatory Commission 32
FedEx Corp. 17
Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security 14
Francophone SAP Users' Club 10
Gartner Inc. 11, 14, 17, 23
General Electric Co. 17
Global Strategic Partners LLC 33
Google Inc. 12, 33, 34
GroundedPower Inc. 20
Heartland Payment Systems Inc. 22
IBM 10, 11
Intermountain Healthcare 17
LifeWatch Corp. 16
Methodist Healthcare System 17
Microsoft Corp. 10, 11, 12, 17, 26
Motorola Inc. 17
National Security Council 33
New York University 18
Nokia Corp. 12
North American Electric Reliability Corp. 30
Oracle Corp. 10, 11
Panasonic Corp. 14
Pathology Associates Medical Laboratories 17
Qualcomm Inc. 11
SANS Institute 26
SAP AG 10
Sarah Jane Brain Foundation Inc. 6
Scripps Health 16
Scripps Translational Science Institute 16
Sharp Corp. 14
Sikalosoft 6
Software Engineering Institute 24
Sony Corp. 14
Sprint Nextel Corp. 17
State Street Global Advisors Inc. 14
Sun Microsystems Inc. 11
SunGard Availability Services LP 14
Telcordia Technologies Inc. 28
Tennessee Valley Authority 32
The Depository Trust & Clearing Corp. 23, 24
The Mitre Corp. 26
The Procter & Gamble Co. 23
Training Camp 37
Trusted Computing Group 26
Twitter Inc. 37
U.S. Centers for Disease Control 40
U.S. Cyber Consequences Unit 32
U.S. Department of Defense 28
U.S. Department of Justice 12
U.S. Government Accountability Office 32
United Parcel Service Inc. 17
Verizon Wireless 17
Vrije Universiteit 12
World Health Organization 14, 40

1&1 Internet C2-1
www.1and1.com
AT&T C3
att.com/laptopconnect
CDW Corporation 13
CDW.com
ESET 3
www.eset.com
Hewlett-Packard C4
hp.com/go/G6superstar6
IBM iT Campaign 9
ibm.com/green/bladecenter
IBM iT Campaign 25
ibm.com/dynamic
IBM iT Campaign 27
ibm.com/intelligent
IBM iT Campaign 29
ibm.com/connected
IBM iT Campaign 31
ibm.com/efficient
iT Innovations Forum 21
virtualconferences.computerworld.com/itinnovations
Microsoft SQL Server 2008 15
SQLServerEnergy.com
SAS 5
www.sas.com/grow
Sprint 7
sprint.com/convergence
Verizon Wireless 19
verizonwireless.com/smallbusiness

This index is provided as an additional service. The publisher does not assume any liability for errors or omissions.

Periodical postage paid at Framingham, Mass., and other mailing offices. Posted under Canadian International Publication agreement PM40063731. **CANADIAN POSTMASTER:** Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A 7C9. Computerworld (ISSN 0010-4841) is published weekly, except for combined issues in November and the last week and first week of each of the following months: December/January, March/April, May/June, June/July, and August/September by Computerworld, Inc., 1 Speen Street, Box 9171, Framingham, Mass. 01701-9171.

Copyright 2009 by Computerworld Inc. All rights reserved. Computerworld can be purchased on microfilm and microfiche through University Microfilms Inc., 300 N. Zeeb Road, Ann Arbor, Mich. 48106. Computerworld is indexed. Back issues, if available, may be purchased from the circulation department. Photocopy rights: permission to photocopy for internal or personal use is granted by Computerworld Inc. for libraries and other users registered with the Copyright Clearance Center (CCC), provided that the base fee of $3 per copy of the article, plus 50 cents per page, is paid directly to Copyright Clearance Center, 27 Congress St., Salem, Mass. 01970. Reprints (minimum 100 copies) and permission to reprint may be purchased from Ray Trynovich, Computerworld Reprints, c/o The YGS Group, Greenfield Corporate Center, 1808 Colonial Village Lane, Lancaster, Pa., 17601, (800) 290-5460, Ext. 148. Fax: (717) 399-8900. Web site: www.reprintbuyer.com. E-mail: computerworld@theygsgroup.com. Requests for missing issues will be honored only if received within 60 days of issue date.

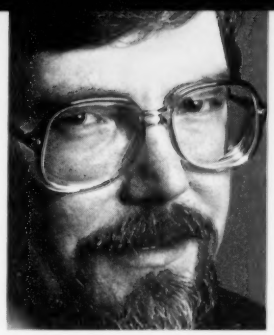
BPA WORLDWIDE ABM

Subscription rates: $5 per copy U.S. – $99.99 per year; Canada – $130 per year; Central & So. America, $250 per year; Europe – $295 per year; all other countries – $296 per year. Subscriptions call toll-free (888) 559-7327. **POSTMASTER:** Send Form 3579 (Change of Address) to Computerworld, PO Box 3500, Northbrook, Ill. 60065-3500.

■ FRANKLY SPEAKING

Frank Hayes

No Panic Required



FED UP with swine flu fearmongers? Feeling suspicious that the people whose bird-flu pandemic predictions didn't pan out are now trying for a second bite at the apple? You should be. Yes, the current swine flu outbreak is a real health problem. In some places, it's also a real economic problem.

But a real problem for IT shops? It's time for a reality check.

First, the health problem: The World Health Organization and the U.S. Centers for Disease Control are concerned about this new strain of flu. They should be. Flu kills people — usually from complications such as pneumonia, usually the elderly, infants or others especially at risk. But *all* flu strains pose a health threat. Every year, flu sends 200,000 Americans to the hospital — and it kills 36,000.

Flu is dangerous. That's why the WHO and the CDC are making all those statements, and why governments are telling their citizens to avoid unnecessary travel to Mexico, where the disease first emerged. This new strain of flu isn't killing its victims wholesale (in contrast, bird flu has killed 60% of those who got it from birds) or even sending them to hospitals in huge numbers. Mostly it appears to be just a bad case of the flu.

That's the first difference from the much-hyped bird flu. Here's the second: This strain of swine flu can be treated effectively with standard influenza drugs, including Tamiflu and Relenza.

In the U.S., there are federal government stockpiles of at least 50 million doses of these drugs. That's about half a million doses for each currently confirmed U.S. case of swine flu. And we can make more.

Yes, we need to be alert. But even if there are more outbreaks in the U.S., this swine flu can be contained here with reasonable precautions (wash your hands frequently, send sick employees home), existing medicines and slightly increased travel controls.

■ What we know for sure about this outbreak of swine flu is that the pandemic panic peddlers have their economics backward.

What about Mexico, with its thousands sick and hundreds dead from swine flu? It turns out that many early reports lumped all respiratory deaths in Mexico City into the "might be swine flu" category. The number of confirmed cases — and the number of confirmed swine-flu deaths — is now believed to be much smaller.

What we know for sure from the situation in Mexico City is that the pandemic panic peddlers have their economics backward. In Mexico City, government orders have shut down restaurants, theaters and other places that pose a risk for spreading flu virus. That's hammering the local economy and idling workers.

The problem isn't that the flu is leaving businesses shorthanded the way pandemic pundits predicted. Instead, shutdowns are leaving businesses unable to afford regular staffing levels.

So there's little likelihood that you'll need to lay in a supply of food, water, fuel and face masks. In practice, you'll be more likely to lay people off than to lock them in.

Where does that leave those of us in U.S. IT shops? In the middle (see story, page 14). It's not a nonevent — swine flu really does pose a potential threat. But it's also not a business crisis we need to throw money at in the middle of a recession.

It's the hardest kind of problem for U.S. businesses: one that requires active monitoring but not immediate, drastic action.

So ignore the fearmongers. Just be vigilant, keep your coughs and sneezes to yourself, and tell your staffers to stay home if they're sick. That's not as exciting as pandemic panic — just the swine flu's challenging reality. ■

Frank Hayes *is Computerworld's senior news columnist. Contact him at frank_hayes@computerworld.com.*

Andy Roddick has the fastest serve in tennis, but Bill Kurtis is faster. *On the Internet.*

With the AT&T 3G LaptopConnect card, download, surf, and stream faster from virtually anywhere on the nation's fastest 3G network.

FREE
AFTER MAIL-IN REBATE
USBConnect Mercury AirCard

Pay $99.99 for card and after mail-in rebate, receive $100 AT&T Promotion Card. $60/mo. DataConnect plan & 2-year svc. agreement required.

MORE BARS IN MORE PLACES™
BEST COVERAGE WORLDWIDE[‡]

at&t
Your world. Delivered.

Go to att.com/laptopconnect or visit your nearest AT&T store.

[‡]The most phones that work in the most countries.

3G not available in all areas. **Coverage** is not available in all areas. See coverage map at stores for details. **Limited-time offer.** Other conditions & restrictions apply. See contract & rate plan brochure for details. Subscriber must live & have a mailing addr. within AT&T's owned wireless network coverage area. **Early Termination Fee:** None if cancelled in the first 30 days, but up to $20 restocking fee may apply to equipment returns; thereafter up to $175. Some agents impose add'l fees. **AT&T Promotion Card:** Allow 60 days for fulfillment. Card request must be postmarked by 7/18/09 & you must be a customer for 30 consecutive days to receive card. DataConnect plan is not unlimited & substantial charges may be incurred if included allowance is exceeded. **Sales tax** calculated based on price of unactivated equipment. ©2009 AT&T Intellectual Property. Service provided by AT&T Mobility. All rights reserved. AT&T, the AT&T logo, and all other marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners.

intel Xeon inside

Powerful. Intelligent.

ALTERNATIVE THINKING ABOUT SERVER ECONOMICS:

Perform like a superstar. Save like an accountant.

Now more than ever, you need your money to work harder. With the new generation of HP ProLiant G6 Servers with Intel® Xeon® processor 5500 series you dramatically improve energy efficiency, flexibility and performance. And more reliability in each system means you can reduce business risk as you increase your productivity.

Decrease your IT support costs to an absolute minimum. HP Insight Control Suite (ICE) will help you to reduce operational expenses by up to $48,380 per 100 users.*

For total peace of mind, HP Care Pack Services deliver industry leading automated 24X7 system monitoring, diagnosis and fault notification to protect your investment.

Making you and your business shine.

Technology for better business outcomes.

HP ProLiant DL360 G6 Server

- Up to two Intel® Xeon® Processor 5500 Series
- 144 GB maximum memory footprint
- Supports up to 8 small form factor high-performance SAS hard drives
- HP ProLiant Onboard Administrator powered by Integrated Lights-Out 2

$2,969 (Save $762)

Lease for just $72/mo.**

Smart Buy [PN:519567-005]

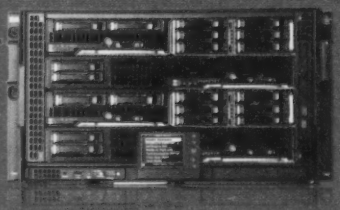
HP ProLiant BL460c G6 Server Blade

- Up to two Intel® Xeon® Processor 5500 Series
- 96 GB maximum memory footprint
- Embedded Dual Port Flex-10 10GbE Multifunction Server Adapter
- HP ProLiant Onboard Administrator powered by Integrated Lights-Out 2

$3,033 (Save $350)

Lease for just $74/mo.**

Smart Buy [PN:532020-B21]



HP BladeSystem c3000 Enclosure

- Supports up to 8 server/storage blade devices in a 6U enclosure
- Optional HP Insight Control Environment management suite
- Low-line or high-line power options for maximum power flexibility

$3,499 (Save $2,319)

Lease for just $85/mo.**

Smart Buy [PN:481657-001]

Special 0% financing for up to 36 months also available.†
To learn more, call 1-866-625-0808 or visit hp.com/go/G6superstar6

hp

*Source: IDC white Paper sponsored by HP, "Gaining Business Value and ROI with HP Insight Control" Document #210479, Feb 2008. **Prices shown are HP Direct prices; reseller and retail prices may vary. Prices shown are subject to change and do not include applicable state and local taxes or shipping to recipient's address. Offers cannot be combined with any other offer or discount and are good while supplies last. All featured offers available in U.S. only. Savings based on HP published list price of configure-to-order equivalent (exclusions: $5,818–$2,319 instant savings = SmartBuy price of $3,499; BL Server: $3,383–$350 instant savings = SmartBuy price of $3,033; DL Server: $3,731–$762 instant savings = SmartBuy price of $2,969. Financing available through Hewlett-Packard Financial Services Company and its subsidiaries (HPFSC) to qualified commercial customers in the U.S. and is subject to credit approval and execution of standard HPFSC documentation. Prices shown are based on a lease 48 months in term with a Fair market value purchase option at the end of the term and are valid through July 31, 2009. Other rates apply for other terms and transaction sizes. Financing is available on transactions greater than $349. Other charges and restrictions may apply. HPFSC reserves the right to change or cancel this program at any time without notice. †Financing available through Hewlett-Packard Financial Services Company and its subsidiaries (HPFSC) to qualified commercial customers in the US and Canada and is subject to credit approval and execution of standard HPFSC documentation. Offer valid through July 31, 2009 on transactions in the United States between $1,500 and $150,000 USD and in Canada between $5,000 CAD and $150,000 CAD. Zero percent financing assumes transaction is documented as a lease with a $1 end-of-term purchase option (or local country equivalent), assuming lessee is not required to pay any nominal end-of-term purchase price or the end of the lease term and disregarding any charges payable by lessee other than rent payments such as maintenance, taxes, fees and shipping. This offer cannot be combined with any other rebate, discount or promotion without prior approval by HP and HPFSC. Rates are based on customer's credit rating, financing terms, offering types, equipment type and options. Not all HP products are eligible for the 0% lease rate. Not all customers may qualify for these rates. Other restrictions may apply. HPFSC reserves the right to change or cancel this program at any time without notice.
Intel, the Intel logo, Xeon and Xeon inside are trademarks of Intel Corporation in the U.S. and other countries.
©2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.